ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Ανάλυση Κυβερνοαπειλών και Προτεινόμενο Μοντέλο Αρχιτεκτονικής Κυβερνοασφάλειας για Συστήματα SCADA

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Φώτιου Σκορδούλη

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2025

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Ανάλυση Κυβερνοαπειλών και Προτεινόμενο Μοντέλο Αρχιτεκτονικής Κυβερνοασφάλειας για Συστήματα SCADA

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Φώτιου Σκορδούλη

Επιβλέπων : Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις 8 Ιουλίου του 2025.

.....	.....	.....
Δημήτριος Ασκούνης Καθηγητής Ε.Μ.Π.	Ιωάννης Ψαρράς Καθηγητής Ε.Μ.Π.	Χρυσόστομος Δούκας Καθηγητής Ε.Μ.Π.

Αθήνα, 8 Ιούλιος 2025

……

Φώτιος Σκορδούλης
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Η ολοένα αυξανόμενη ανάγκη για αυτοματοποίηση σε κρίσιμες υποδομές, όπως η ενέργεια, οι μεταφορές και η ύδρευση, έχει οδηγήσει στην ευρεία χρήση των συστημάτων SCADA (Supervisory Control and Data Acquisition). Τα συστήματα αυτά επιτρέπουν την απομακρυσμένη παρακολούθηση και τον έλεγχο φυσικών διεργασιών σε πραγματικό χρόνο. Ωστόσο, η τεχνολογική πρόοδος συνοδεύεται και από νέες προκλήσεις, με κυριότερη τον αυξανόμενο κίνδυνο στον τομέα της κυβερνοασφάλειας. Η δικτυακή διασύνδεση των SCADA με εξωτερικά δίκτυα ή δίκτυα χωρίς κατάλληλη απομόνωση ή ασφάλεια καθιστά τις υποδομές αυτές ευάλωτες σε κυβερνοεπιθέσεις, οι οποίες ενδέχεται να έχουν σοβαρές επιπτώσεις στη λειτουργικότητα, την ασφάλεια και την οικονομική βιωσιμότητα οργανισμών και κρατικών δομών.

Η ανάγκη για εποπτεία σε πραγματικό χρόνο, αποκεντρωμένη ανάλυση, ταχεία απόκριση και αξιοποίηση της συσσωρευμένης γνώσης από παλαιότερα περιστατικά, καθιστά αναγκαία την υιοθέτηση μιας νέας αρχιτεκτονικής προσέγγισης. Η παρούσα εργασία έρχεται να καλύψει αυτό το κενό, προτείνοντας ένα σύγχρονο μοντέλο που βασίζεται σε κατανεμημένη επεξεργασία συστημάτων SIEM (Security Information and Event Management), δηλαδή εργαλείων ανίχνευσης και διαχείρισης συμβάντων ασφαλείας, ενσωμάτωση τεχνικών τεχνητής νοημοσύνης για εμπλουτισμένη ανάλυση απειλών και ένα σύστημα διαχείρισης γνώσης (Knowledge Management Layer) για την επιχειρησιακή αξιοποίηση των δεδομένων ασφαλείας.

Η προτεινόμενη αρχιτεκτονική στοχεύει στη βελτίωση της ακρίβειας εντοπισμού επιθέσεων, την αποκέντρωση της ανάλυσης για καλύτερη επεκτασιμότητα, και την υποστήριξη του αναλυτή με τεκμηριωμένες πληροφορίες και προτεινόμενες ενέργειες απόκρισης. Ο σχεδιασμός της βασίστηκε σε απαιτήσεις πραγματικών περιβαλλόντων SCADA και σε σενάρια επιθέσεων που συναντώνται στη βιβλιογραφία, ώστε να είναι κατάλληλη για μελλοντική αξιολόγηση. Μέσα από αυτή την προσέγγιση, ενισχύεται η δυνατότητα πρόληψης, απόκρισης και τεκμηρίωσης, συμβάλλοντας στην ανθεκτικότητα των κρίσιμων υποδομών απέναντι σε σύγχρονες και εξελιγμένες κυβερνοαπειλές.

Λέξεις Κλειδιά: Βιομηχανικά Συστήματα ελέγχου, SCADA, IoT, Big Data Analytics, CAPEC, CWE, Mitre Att&ck, HDFS, Κυβερνοασφάλεια, διερεύνηση απειλών

Abstract

The ever-increasing need for automation in critical infrastructures such as energy, transportation, and water supply has led to the widespread use of SCADA systems (Supervisory Control and Data Acquisition). These systems enable remote monitoring and control of physical processes in real time. However, technological advancement also brings new challenges, the most significant being the growing risk in the field of cybersecurity. The network interconnection of SCADA systems with external or improperly isolated networks makes these infrastructures vulnerable to cyberattacks, which may have serious impacts on the functionality, safety, and economic viability of organizations and public services.

The need for real-time supervision, decentralized analysis, rapid response, and the utilization of accumulated knowledge from past incidents highlights the necessity for a new architectural approach. This thesis addresses that gap by proposing a modern model based on distributed processing of SIEM (Security Information and Event Management) systems—tools for detecting and managing security incidents—combined with artificial intelligence techniques for enriched threat analysis and a Knowledge Management Layer for the operational utilization of security data.

The proposed architecture aims to improve the accuracy of attack detection, decentralize analysis for better scalability, and support analysts with well-documented information and recommended response actions. Its design was based on the requirements of real SCADA environments and attack scenarios found in the literature, making it suitable for future evaluation. Through this approach, prevention, response, and documentation capabilities are enhanced, contributing to the resilience of critical infrastructures against modern and advanced cyber threats.

Keywords: Industrial automatic control systems, SCADA, IoT, Big Data Analytics, CAPEC, CWE, Mitre Att&ck, HDFS, cybersecurity, digital forensic investigation.

Ευχαριστίες

Η εκπόνηση της παρούσας διπλωματικής εργασίας πραγματοποιήθηκε στο εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης του τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών Ε.Μ.Π..

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Ασκούνη Δημήτριο για την ανάθεση του συγκεκριμένου θέματος και την δυνατότητα που μου δόθηκε να γνωρίσω νέα επιστημονικά δεδομένα και τεχνολογίες. Τις ευχαριστίες μου επίσης στους καθηγητές κ. Ψαρρά Ιωάννη και κ. Δούκα Χρυσόστομο, για την παρουσία τους στην τριμελή εξεταστική επιτροπή.

Ιδιαίτερες ευχαριστίες θα ήθελα να δώσω στην συνεπιβλέπουσα Μιχαλίτση-Ψαρρού Αριάδνη για την καίρια καθοδήγηση και συνεργασία κατά την εκπόνηση της εργασίας. Τέλος θα ήθελα να ευχαριστήσω τους δικούς μου ανθρώπους και την οικογένεια μου για την στήριξη και συμπαράσταση καθ' όλη την διάρκεια των σπουδών.

Φώτιος Σκορδούλης

Ιούλιος 2025

Πίνακας περιεχομένων

Περίληψη **5**

Abstract **7**

Ευχαριστίες **9**

Πίνακας περιεχομένων **10**

1 Εισαγωγή **13**

1.1 Η σημασία και η ανάγκη προστασίας των συστημάτων SCADA **14**

1.2 Αντικείμενο διπλωματικής **15**

1.3 Οργάνωση κειμένου **16**

2 Ανασκόπηση Σχετικής Βιβλιογραφίας Συστημάτων SCADA και Προσεγγίσεων Κυβερνοασφάλειας **18**

2.1 Ανάλυση συστημάτων SCADA **18**

2.1.1 Ορισμός και Λειτουργία των Συστημάτων SCADA 18

2.1.2 Στοιχεία Συστημάτων SCADA 19

2.2 Ο Ρόλος των Συστημάτων SCADA στις Κρίσιμες Υποδομές **27**

2.3 Κυβερνοαπειλές και Τρωτά Σημεία στα συστήματα SCADA **28**

2.3.1 Γενικές Απειλές και Προκλήσεις 28

2.3.2 Κατηγοριοποίηση Τρωτών Σημείων 29

2.4 Ψηφιακή Εγκληματολογική διερεύνηση Κυβερνοεπιθέσεων στα συστήματα SCADA **32**

2.4.1 Σκοπός και Σημασία της Ψηφιακής Εγκληματολογικής Διερεύνησης 32

2.4.2 Τυπικά στάδια Ψηφιακής Εγκληματολογικής διερεύνησης 34

2.4.3 Κριτήρια και μεθοδολογίες ταξινόμησης απειλών στην κυβερνοασφάλεια 38

2.5 Αρχιτεκτονική Συστημάτων Ασφαλείας **42**

2.6 Εργαλεία διερεύνησης Κυβερνοεπιθέσεων **44**

2.6.1 Γενικές παρατηρήσεις 44

2.6.2 Συστήματα SIEM: Συλλογή και Ανάλυση Δεδομένων Ασφαλείας 45

2.6.3 Βάσεις Γνώσης για την Ψηφιακή Εγκληματολογική Διερεύνηση Κυβερνοαπειλών 48

2.6.4 Αποθήκευση και Ανάλυση Μεγάλων Δεδομένων με HDFS 49
2.6.5 Automated Forensic Tool: Πολυεπίπεδο Εργαλείο Ανάλυσης Συμβάντων Ασφαλείας 52

3 Προτεινόμενη αρχιτεκτονική 55

3.1 Σκοπός και βασικές αρχές 55

3.2 Δομικά Στοιχεία 56

3.2.1 Συσκευές Πεδίου και Ελεγχόμενος Εξοπλισμός 56
3.2.2 Κεντρικό Σύστημα Ελέγχου 56
3.2.3 Υποσύστημα Δικτυακής Επικοινωνίας 57
3.2.4 Wazuh – Σύστημα Ανίχνευσης και Ανάλυσης Συμβάντων 58
3.2.5 HDFS – Σύστημα Αποθήκευσης και Ανάλυσης Δεδομένων – 59
3.2.6 Automated Forensic Tool – Σύστημα Υποστήριξης Εγκληματολογικής Ανάλυσης 60
3.2.7 Σύνοψη των Δομικών Επιλογών 61

3.3 Περιγραφή και Δομή αρχιτεκτονικής 62

3.3.1 Field Layer: Συλλογή και Τοπική Ανάλυση 64
3.3.2 Network Layer: Επικοινωνία και Ασφάλεια 64
3.3.3 Control Layer: Συγκέντρωση και Διαχείριση Δεδομένων 64
3.3.4 AI & Forensic Processing Layer: Ευφυής Ανάλυση και Αυτοματοποιημένη Διερεύνηση 66
3.3.5 Knowledge Management Layer: Συγκέντρωση Πληροφοριών συμβάντων ασφαλείας 67

3.4 Σενάριο Χρήσης: Ανίχνευση και Αντιμετώπιση Κυβερνοεπιθέσεων 68

3.5 Καινοτομία της Προτεινόμενης Αρχιτεκτονικής 70

3.6 Σύγκριση Υφιστάμενων Αρχιτεκτονικών Κυβερνοασφάλειας σε SCADA . 71

3.6.1 Σύγκριση φυσικών υποδομών SCADA 72
3.6.2 Σύγκριση λύσεων στην διαχείριση συμβάντων ασφαλείας SCADA 78

4 Συμπεράσματα και Μελλοντικές Προεκτάσεις 85

Βιβλιογραφία 88

Κατάλογος Εικόνων

Εικόνα 2.1-i: Βασική αρχιτεκτονική SCADA. Πηγή: www.researchgate.net.....20
Εικόνα 2.1-ii: Programmable Logic Controller. Πηγή: worktech.gr.....22
Εικόνα 2.1-iii: Remote Terminal Unit. Πηγή: wikipedia.org.....23
Εικόνα 2.1-iv: Intelligent Electronic Device. Πηγή: electrical-engineering-portal.com 24
Εικόνα 2.6-i: Συσχέτιση πλαισίων MITRE ATT&CK, CAPEC και CWE για την ανάλυση κυβερνοεπιθέσεων. Πηγή: nopsec.com 49
Εικόνα 2.6-ii: Αρχιτεκτονική του HDFS (Hadoop Distributed File System). Πηγή: medium.com.....52
Εικόνα 3.2-i: Αρχιτεκτονική Wazuh. Πηγή: wazuh 58
Εικόνα 3.2-ii: Πίνακας Ελέγχου Wazuh. Πηγή: wazuh.....59
Εικόνα 3.3-i: Δομή της προτεινόμενης αρχιτεκτονικής.....63

Κατάλογος Πινάκων

Πίνακας 2.6-i: Συγκριτικός Πίνακας για την επιλογή SIEM.....48
Πίνακας 3.6-i: Συγκριτικός Πίνακας αξιολογήσεων στην διαχείριση συμβάντων ασφαλείας SCADA.....84

1 *Εισαγωγή*

Η αρχιτεκτονική κυβερνοασφάλειας για συστήματα SCADA (Supervisory Control and Data Acquisition) αποτελεί έναν από τους πιο κρίσιμους τομείς της σύγχρονης τεχνολογίας, καθώς η προστασία αυτών των συστημάτων από κυβερνοεπιθέσεις είναι ζωτικής σημασίας για την ασφάλεια των υποδομών και των κρίσιμων λειτουργιών σε διάφορους τομείς, όπως η ενέργεια, οι μεταφορές, οι τηλεπικοινωνίες και η βιομηχανία. Τα συστήματα SCADA χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο βιομηχανικών διαδικασιών σε πραγματικό χρόνο, επιτρέποντας στους χρήστες να ελέγχουν εξοπλισμό, να συλλέγουν δεδομένα και να αυτοματοποιούν λειτουργίες σε ένα μεγάλο φάσμα εφαρμογών.

Ωστόσο, με την αύξηση της σύνδεσης αυτών των συστημάτων στο διαδίκτυο και σε άλλες δικτυωμένες υποδομές, τα συστήματα SCADA έχουν καταστεί ευάλωτα σε επιθέσεις από κακόβουλους παράγοντες. Οι κυβερνοεπιθέσεις μπορούν να έχουν καταστροφικές συνέπειες, όπως την αποδιοργάνωση λειτουργιών, την απώλεια ή υποκλοπή κρίσιμων δεδομένων, ακόμη και την παραβίαση της ασφάλειας και της ακεραιότητας της υποδομής.

Η αρχιτεκτονική κυβερνοασφάλειας για τα συστήματα SCADA πρέπει να περιλαμβάνει πολυδιάστατες στρατηγικές που συνδυάζουν τεχνολογίες, διαδικασίες και πολιτικές με σκοπό την πρόληψη, ανίχνευση και ανθεκτικότητα απέναντι σε επιθέσεις. Αυτές οι στρατηγικές περιλαμβάνουν τη χρήση προηγμένων μηχανισμών κρυπτογράφησης, την παρακολούθηση της δικτυακής κυκλοφορίας, την ενίσχυση της φυσικής ασφάλειας των συσκευών SCADA και την εφαρμογή πολιτικών πρόσβασης που περιορίζουν την εξουσιοδότηση.

Επιπλέον, η συνεχιζόμενη εκπαίδευση του προσωπικού, η ανάπτυξη σχεδίων έκτακτης ανάγκης και η συνεχής ανανέωση των συστημάτων ασφαλείας είναι εξίσου σημαντικές για την αποτελεσματική διαχείριση των κινδύνων. Η εργασία αυτή επικεντρώνεται στην ανάλυση των διαφόρων παραμέτρων της αρχιτεκτονικής κυβερνοασφάλειας των συστημάτων SCADA, καθώς και στην αναγνώριση και προτάσεις βελτίωσης για την προστασία αυτών των κρίσιμων υποδομών.

1.1 Η σημασία και η ανάγκη προστασίας των συστημάτων SCADA

Το σύστημα SCADA (Supervisory Control And Data Acquisition) είναι μια αρχιτεκτονική συστήματος βιομηχανικού αυτόματου ελέγχου και τηλεμετρίας που χρησιμοποιείται για την παρακολούθηση και τον έλεγχο διεργασιών σε πραγματικό χρόνο. Το χαρακτηριστικό των συστημάτων SCADA είναι ότι αποτελούνται από συσκευές πεδίου (Field devices) που συνδέονται σε ένα κεντρικό σύστημα ελέγχου (Control center). Οι συσκευές πεδίου είναι υπεύθυνες για τον έλεγχο των επιμέρους μηχανημάτων ενώ το κεντρικό σύστημα ελέγχου συλλέγει και επεξεργάζεται τα δεδομένα των συσκευών πεδίου. Τα συστήματα SCADA είναι υπεύθυνα για την παρακολούθηση, τον αυτοματισμό και τον έλεγχο πολλών κρίσιμων υποδομών παγκοσμίως. [6]

Οι επιθέσεις σε υποδομές ζωτικής σημασίας έχουν αυξηθεί όλα αυτά τα χρόνια όπως δείχνουν σχετικές εκθέσεις και έρευνες. Ήδη από το 2012 υπήρξαν 198 επιθέσεις εναντίον βιομηχανιών, υποδομών κοινής ωφέλειας και άλλων κρίσιμων εγκαταστάσεων. Αυτού του είδους οι επιθέσεις γίνονται ολοένα πιο περίπλοκες με στόνο την κατασκοπεία και τη δολιοφθορά ενώ παράλληλα αυξάνονται οι επιθέσεις που σχετίζονται με το κυβερνοέγκλημα [24]. Δεν είναι πια καθόλου σπάνιο τα κακόβουλα λογισμικά να χρησιμοποιηθούν για την κατασκοπεία στον κυβερνοχώρο, που συχνά αφορά τον ενεργειακό τομέα, με στόχο τη συλλογή ευαίσθητων πληροφοριών [3]. Επίσης, η αυξημένη πολυπλοκότητα των κυβερνοεπιθέσεων συχνά οδηγεί στην καταστροφή των συστημάτων που έχουν δεχθεί επίθεση καθιστώντας δύσκολη την εγκληματολογική ανάλυση. Αυτό συμβαίνει επειδή, κατά τον αρχικό τους σχεδιασμό, οι κρίσιμες αυτές υποδομές δεν επικεντρώνονταν στην ασφάλεια και την προστασία τους από κακόβουλες επιθέσεις [18].

Μέχρι να αρχίσουν να αναπτύσσονται τα συστήματα SCADA, η βιομηχανία και οι υποδομές εστίαζαν στην διαθεσιμότητα των δεδομένων παρά στην εμπιστευτικότητα και διαφύλαξή τους από κακόβουλες επιθέσεις και απειλές, που στην πορεία και μέχρι σήμερα όλο και μεγαλώνουν με την ανάπτυξη του διαδικτύου [16]. Ακόμα και σήμερα πολλές υποδομές ζωτικής σημασίας είναι παρωχημένες, εξακολουθούν να λειτουργούν με παλιά λειτουργικά συστήματα ή δεν ενημερώνουν όσο συχνά πρέπει τον κώδικα

(ειδικά σε μη αναπτυγμένες χώρες) με αποτέλεσμα να αποτελούν εύκολο στόχο για κακόβουλα λογισμικά, απειλές και γενικά κυβερνοεπιθέσεις [7].

Με την εκθετική ανάπτυξη των δυνατοτήτων δικτύωσης, το διαδίκτυο επηρεάζει πλέον σχεδόν κάθε πτυχή της κοινωνικής ζωής. Αυτό έχει οδηγήσει σε ένα ξέσπασμα απειλών στον κυβερνοχώρο που πραγματοποιούνται από κυβερνοεγκληματίες. Ενδεικτικά, το 2020 αναφέρθηκαν περισσότερες κυβερνοεπιθέσεις από οποιαδήποτε άλλη χρονιά. Έτσι, η ανάγκη προστασίας των συστημάτων πληροφορικής έχει γίνει κρίσιμη στις μέρες μας ιδιαίτερα για ανεπτυγμένες χώρες στον τομέα της τεχνολογίας που αντιμετωπίζουν περισσότερες απειλές.

Η ανταλλαγή γνώσης αλλά και πληροφοριών σχετικά με τις αδυναμίες που μπορεί να παρουσιάζονται στα συστήματα είναι υψίστης σημασίας για την πρόληψη απειλών και επιθέσεων στον τομέα της κυβερνοασφάλειας [13]. Η αποτελεσματική διαχείριση των αδυναμιών των συστημάτων είναι εξίσου ή και ακόμα πιο σημαντική από τις δοκιμές νέων προϊόντων ή λογισμικών. Επιπλέον, η έρευνα και ανάπτυξη συστημάτων για τον εντοπισμό αυτών των αδυναμιών είναι απαραίτητα στοιχεία για την αντιμετώπιση των κυβερνοεπιθέσεων σε κρίσιμους τομείς της βιομηχανίας και των υποδομών [20].

1.2 Αντικείμενο διπλωματικής

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η μελέτη των σύγχρονων προσεγγίσεων στον τομέα της κυβερνοασφάλειας για βιομηχανικά συστήματα SCADA, καθώς και η πρόταση μιας νέας αρχιτεκτονικής που θα μπορεί να ανταποκριθεί αποτελεσματικά στις αυξημένες απαιτήσεις παρακολούθησης, ανίχνευσης και απόκρισης σε επιθέσεις.

Η εργασία περιλαμβάνει μια εκτενή θεωρητική επισκόπηση των βασικών δομικών στοιχείων ενός συστήματος SCADA, των τύπων απειλών που το στοχεύουν και των μεθόδων που χρησιμοποιούνται για την ενίσχυση της ασφάλειάς του. Παράλληλα, μελετώνται σύγχρονες τεχνολογικές τάσεις όπως η κατανεμημένη επεξεργασία δεδομένων, η ανάλυση περιστατικών με τη χρήση τεχνητής νοημοσύνης και οι προσεγγίσεις ψηφιακής εγκληματολογικής διερεύνησης που εφαρμόζονται σε κρίσιμες υποδομές.

Στην συνέχεια, η εργασία προτείνει μια νέα αρχιτεκτονική ασφάλειας, η οποία συνδυάζει επιμέρους τεχνολογίες και λειτουργικά επίπεδα σε ένα ενιαίο σχήμα. Στόχος είναι η ενίσχυση της ακρίβειας εντοπισμού των επιθέσεων, η αποκέντρωση της ανάλυσης για καλύτερη επεκτασιμότητα, καθώς και η διατήρηση και αξιοποίηση της παραγόμενης γνώσης για την υποστήριξη της απόκρισης σε μελλοντικά περιστατικά.

1.3 Οργάνωση κειμένου

Η παρούσα διπλωματική εργασία οργανώνεται σε τρία βασικά κεφάλαια. Στο πρώτο κεφάλαιο παρουσιάζεται το γενικό πλαίσιο της έρευνας, επισημαίνεται η σημασία της κυβερνοασφάλειας στα συστήματα SCADA και περιγράφεται ο σκοπός της μελέτης.

Το δεύτερο κεφάλαιο αποτελεί το θεωρητικό υπόβαθρο της εργασίας και επικεντρώνεται στην εκτενή βιβλιογραφική επισκόπηση του τομέα της κυβερνοασφάλειας στα συστήματα SCADA. Αρχικά, γίνεται αναφορά στη δομή, τη λειτουργία και τις βασικές συνιστώσες των SCADA, με στόχο την κατανόηση του τρόπου με τον οποίο επιτελούν τον ρόλο τους σε κρίσιμες υποδομές. Στη συνέχεια, αναλύονται οι απειλές και τα τρωτά σημεία που εντοπίζονται σε τέτοια συστήματα, λαμβάνοντας υπόψη τις ιδιαιτερότητες των βιομηχανικών περιβαλλόντων, όπως η ανάγκη για διαθεσιμότητα, σταθερότητα και περιορισμένες δυνατότητες αναβάθμισης. Παρουσιάζονται οι μεθοδολογίες ψηφιακής εγκληματολογικής διερεύνησης κυβερνοεπιθέσεων, με έμφαση στα στάδια της ανάλυσης, της ανίχνευσης, και της τεκμηρίωσης περιστατικών ασφαλείας. Επιπλέον, εξετάζονται τα κύρια εργαλεία που χρησιμοποιούνται στη διερεύνηση και απόκριση, όπως τα συστήματα SIEM (Security Information and Event Management), οι βιβλιοθήκες επιθέσεων και τρωτών σημείων, και τα συστήματα αποθήκευσης και επεξεργασίας μεγάλων δεδομένων, με ιδιαίτερη αναφορά στο HDFS. Τέλος, παρουσιάζονται οι βασικές αρχές της αρχιτεκτονικής ασφάλειας, καθώς και η αξιοποίηση τεχνικών τεχνητής νοημοσύνης για την ανάλυση και την κατηγοριοποίηση κυβερνοαπειλών, θέτοντας το πλαίσιο για τη διαμόρφωση της προτεινόμενης αρχιτεκτονικής που αναπτύσσεται στο επόμενο κεφάλαιο.

Το τρίτο κεφάλαιο αποτελεί τον κορμό της διπλωματικής εργασίας, καθώς παρουσιάζεται η προτεινόμενη αρχιτεκτονική για την ενίσχυση της κυβερνοασφάλειας σε περιβάλλοντα SCADA. Αρχικά, γίνεται αναφορά στις βασικές αρχές και τους στόχους που διέπουν τη σχεδίαση του μοντέλου, ενώ στη συνέχεια περιγράφονται αναλυτικά τα επιμέρους δομικά στοιχεία της αρχιτεκτονικής. Επιπλέον, μέσω ενός

σεναρίου χρήσης, αποτυπώνεται ο τρόπος με τον οποίο η αρχιτεκτονική λειτουργεί στην πράξη κατά τη διάρκεια μιας κυβερνοεπίθεσης, ενισχύοντας τη βιωσιμότητα της πρότασης.

Τέλος, στο τέταρτο κεφάλαιο παρουσιάζονται τα βασικά συμπεράσματα που προκύπτουν από τη μελέτη και την ανάλυση της αρχιτεκτονικής. Γίνεται αποτίμηση της αποτελεσματικότητας της προτεινόμενης προσέγγισης, ενώ παράλληλα διατυπώνονται προτάσεις για μελλοντική έρευνα και επέκταση της παρούσας εργασίας.

2 *Ανασκόπηση Σχετικής Βιβλιογραφίας Συστημάτων SCADA και Προσεγγίσεων Κυβερνοασφάλειας*

2.1 Ανάλυση συστημάτων SCADA

2.1.1 Ορισμός και Λειτουργία των Συστημάτων SCADA

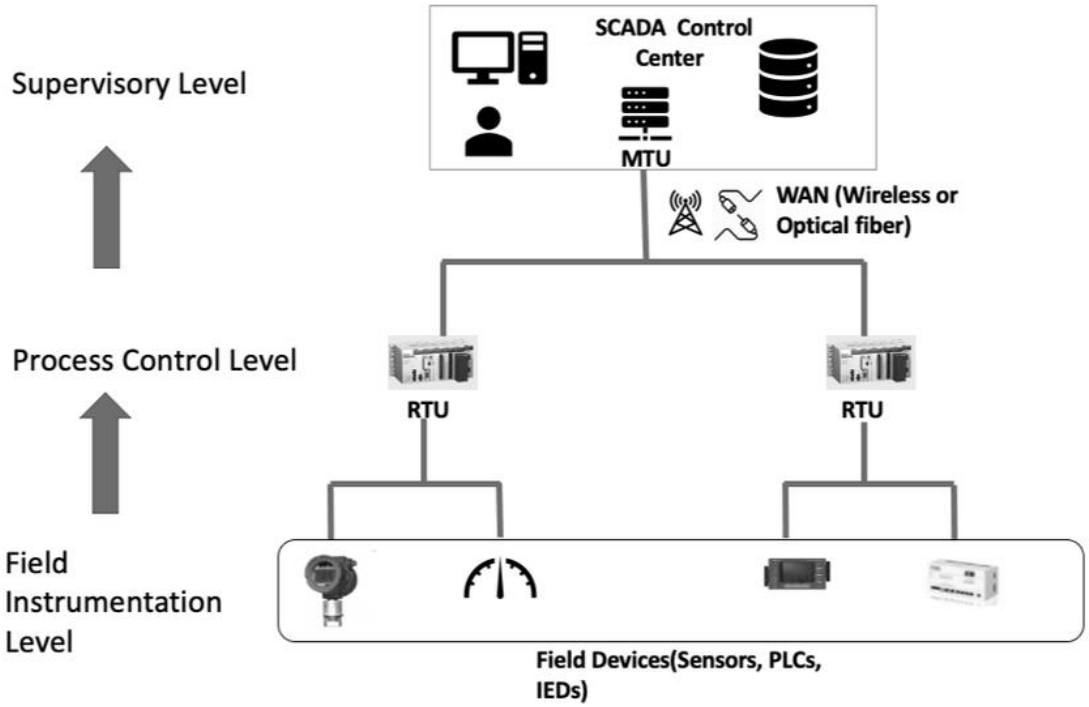
Τα συστήματα SCADA χρησιμοποιούνται κυρίως για την συλλογή δεδομένων σε πραγματικό χρόνο από απομακρυσμένες συσκευές, διευκολύνοντας την αυτοματοποίηση και τον έλεγχο εξοπλισμού [2]. Η σημασία των συστημάτων SCADA έγκειται στη δυνατότητά τους να συλλέγουν δεδομένα από απομακρυσμένες τοποθεσίες, τα οποία χρησιμοποιούνται για τον έλεγχο περιβαλλοντικών συνθηκών. Για παράδειγμα, το SCADA μπορεί να εντοπίσει και να καταγράψει δεδομένα σχετικά με διαρροές σε υποδομές αγωγών. Επιπλέον, αναλύει τα δεδομένα σε πραγματικό χρόνο και ειδοποιεί τον χρήστη για την άμεση αντιμετώπιση τέτοιων περιστατικών. Στα παλαιότερα συστήματα SCADA, δεν απαιτούνταν σύνδεση στο διαδίκτυο, γεγονός που τα καθιστούσε απομονωμένα από δημόσια δίκτυα [23]. Τα τελευταία χρόνια, τα συστήματα SCADA έχουν εξελιχθεί παράλληλα με την πρόοδο της τεχνολογίας, αξιοποιώντας το διαδίκτυο για τη λειτουργία τους. Ωστόσο, η χρήση του διαδικτύου έχει αναδείξει την ανάγκη διερεύνησης της ευπάθειας των υποδομών τους σε πιθανές κυβερνοεπιθέσεις.

Τα συστήματα SCADA έχουν σημειώσει ταχεία ανάπτυξη στην ανταγωνιστική αγορά της τεχνολογίας με έμφαση στην απόδοση. Ωστόσο, τα τρωτά σημεία τους στον τομέα της ασφάλειας πληροφοριών έχουν μελετηθεί εκτενώς, αποδεικνύοντας την ευπάθεια τους σε κυβερνοαπειλές [10]. Σε περίπτωση συμβάντος ασφαλείας (π.χ. αποτυχία συστήματος, παραβίαση ασφάλειας ή επίθεση), είναι σημαντικό να κατανοήσουμε τι γίνεται και ποιες είναι οι ψηφιακές συνέπειες τέτοιων περιστατικών όπως και ποιες διαδικασίες ή πρωτόκολλα χρειάζεται να χρησιμοποιηθούν κατά τη διάρκεια μιας έρευνας, ποια εργαλεία και τεχνικές είναι κατάλληλα να χρησιμοποιηθούν από έναν ερευνητή, και από πού μπορούν να συλλεχθούν τα σχετικά δεδομένα και πώς [10]. Σε περίπτωση συμβάντος ασφαλείας (π.χ. επίθεση πλημμύρας IP(IP flood attack)), είναι σημαντικό να κατανοήσουμε κατά την ψηφιακή εγκληματολογική διερεύνηση ποιες είναι οι συνέπειες μιας τέτοιας επίθεσης. Ποιες

είναι οι διαδικασίες ή τι πρωτόκολλα χρειάζεται να χρησιμοποιηθούν κατά τη διάρκεια μιας έρευνας; Ποια εργαλεία και τεχνικές είναι κατάλληλα για να χρησιμοποιήσει ο ερευνητής; Πού μπορούν να συλλεχθούν σχετικά δεδομένα και πώς; Σε αυτόν τον τομέα, υπάρχει ακόμα ένα σοβαρό κενό στη βιβλιογραφία καθώς η ανάλυση μιας κυβερνοεπίθεσης από τους ερευνητές καθοδηγείται συνήθως από την εμπειρία και τη διαίσθηση του ερευνητή παρά είναι αποτέλεσμα μιας συστηματικής ή επιστημονικής διαδικασίας [28].

2.1.2 Στοιχεία Συστημάτων SCADA

Τα συστήματα SCADA αποτελούνται από μια σειρά επιμέρους τεχνολογικών υποσυστημάτων, καθένα από τα οποία επιτελεί καθοριστικό ρόλο στην παρακολούθηση, τον έλεγχο και την αυτοματοποίηση κρίσιμων διαδικασιών. Η ορθή λειτουργία ενός SCADA εξαρτάται από την αποδοτική συνεργασία μεταξύ των φυσικών συσκευών πεδίου, του κεντρικού συστήματος ελέγχου και των δικτύων επικοινωνίας που τα διασυνδέουν. Η βασική αρχιτεκτονική των συστημάτων SCADA είναι:



Εικόνα 2.1-i: Βασική αρχιτεκτονική SCADA. Πηγή: www.researchgate.net[1]

2.1.2.1 Συσκευές πεδίου

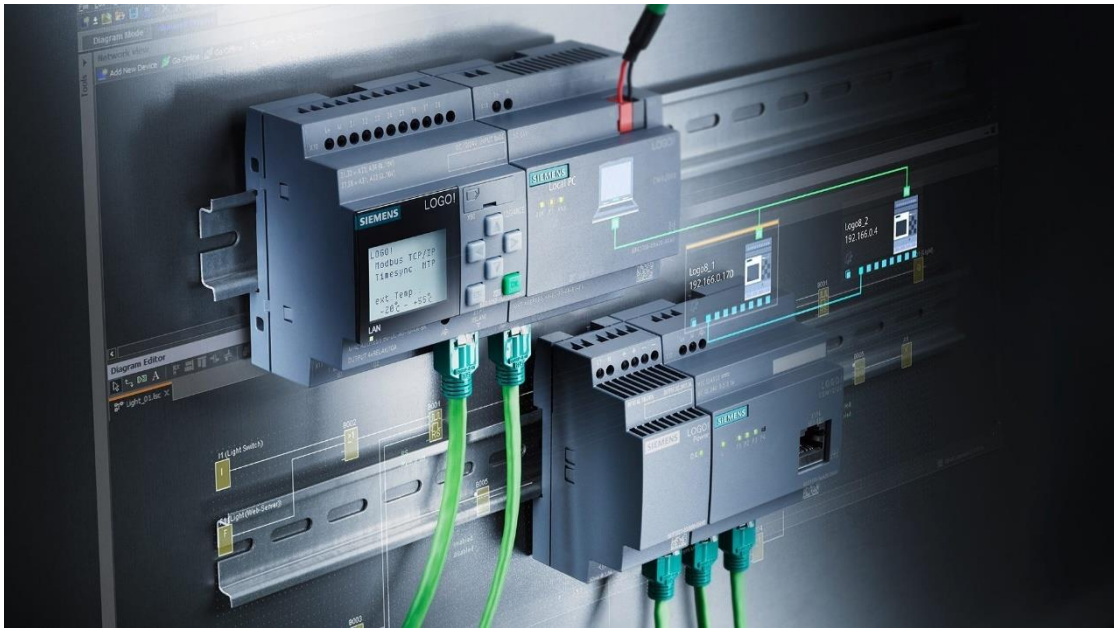
Οι συσκευές πεδίου αποτελούν σημαντικό μέρος των συστημάτων SCADA και είναι υπεύθυνα για την ανίχνευση και την παρακολούθηση φυσικών διεργασιών και τη μετάδοση αυτών των δεδομένων στο κεντρικό σύστημα ελέγχου για περαιτέρω επεξεργασία. Μπορεί να περιλαμβάνουν αισθητήρες, ενεργοποιητές, πομπούς και άλλο εξοπλισμό που χρησιμοποιείται για την παρακολούθηση και τον έλεγχο βιομηχανικών διεργασιών [28]. Συνήθως βρίσκονται σε σκληρό και απομακρυσμένο περιβάλλον, όπως εξέδρες άντλησης πετρελαίου, μονάδες παραγωγής ηλεκτρικής ενέργειας και εγκαταστάσεις επεξεργασίας νερού. Για αυτόν τον λόγο, οι συσκευές πεδίου πρέπει να είναι σχεδιασμένες ώστε να αντέχουν σε σκληρές περιβαλλοντικές συνθήκες και να λειτουργούν αξιόπιστα σε αυτές τις ρυθμίσεις. Πρέπει επίσης να είναι σε θέση να μεταδίδουν δεδομένα με ακρίβεια και σε πραγματικό χρόνο στο κεντρικό σύστημα ελέγχου.

[1] https://www.researchgate.net/figure/Block-diagram-of-a-SCADA-systemMTU-Master-Terminal-Unit-RTUs-Remote-Terminal-Units_fig1_379062622

Για να διασφαλιστεί η ασφάλεια του συστήματος, οι συσκευές πεδίου πρέπει να προστατεύονται από τις παραβιάσεις και τις επιθέσεις και τη με εξουσιοδοτημένη πρόσβαση. Η τακτική συντήρηση και η δοκιμή των συσκευών πεδίου είναι ουσιαστικής σημασίας για τη διασφάλιση της αποτελεσματικής και ασφαλούς λειτουργίας. Αυτό μπορεί να περιλαμβάνει επιθεωρήσεις ρουτίνας, δοκιμές αισθητήρων και συνδέσμων επικοινωνίας και διασφάλιση ότι το λογισμικό και το υλικό είναι ενημερωμένα και διορθωμένα έναντι γνωστών τρωτών σημείων [27]. Είναι επίσης σημαντικό να υπάρχουν σχέδια έκτακτης ανάγκης για τυχόν αστοχίες ή δυσλειτουργίες, συμπεριλαμβανομένων των εφεδρικών συστημάτων για να διασφαλιστεί η συνέχεια των λειτουργιών.

Τα τρία χαρακτηριστικά συστήματα που μπορούν να βοηθήσουν είναι:

1. Programmable Logic Controller (PLC): είναι ένας εξειδικευμένος υπολογιστής που χρησιμοποιείται για τον έλεγχο των διαδικασιών αυτοματισμού σε βιομηχανικά περιβάλλοντα. Τα PLC συνήθως προγραμματίζονται χρησιμοποιώντας τη λογική ladder, μια γραφική γλώσσα προγραμματισμού που επιτρέπει στους μηχανικούς και τους τεχνικούς να σχεδιάζουν πολύπλοκα συστήματα ελέγχου χωρίς την ανάγκη εκτεταμένης γνώσης κωδικοποίησης [24]. Μπορούν να συνδέονται με μια μεγάλη ποικιλία αισθητήρων και ενεργοποιητών, όπως αισθητήρες θερμοκρασίας, αισθητήρες πίεσης και κινητήρες, επιτρέποντάς τους να εκτελούν πολύπλοκες εργασίες ελέγχου, όπως ρύθμιση θερμοκρασίας, πίεσης και ρυθμών ροής.



Εικόνα 2.1-ii: Programmable Logic Controller. Πηγή: worktech.gr[2]

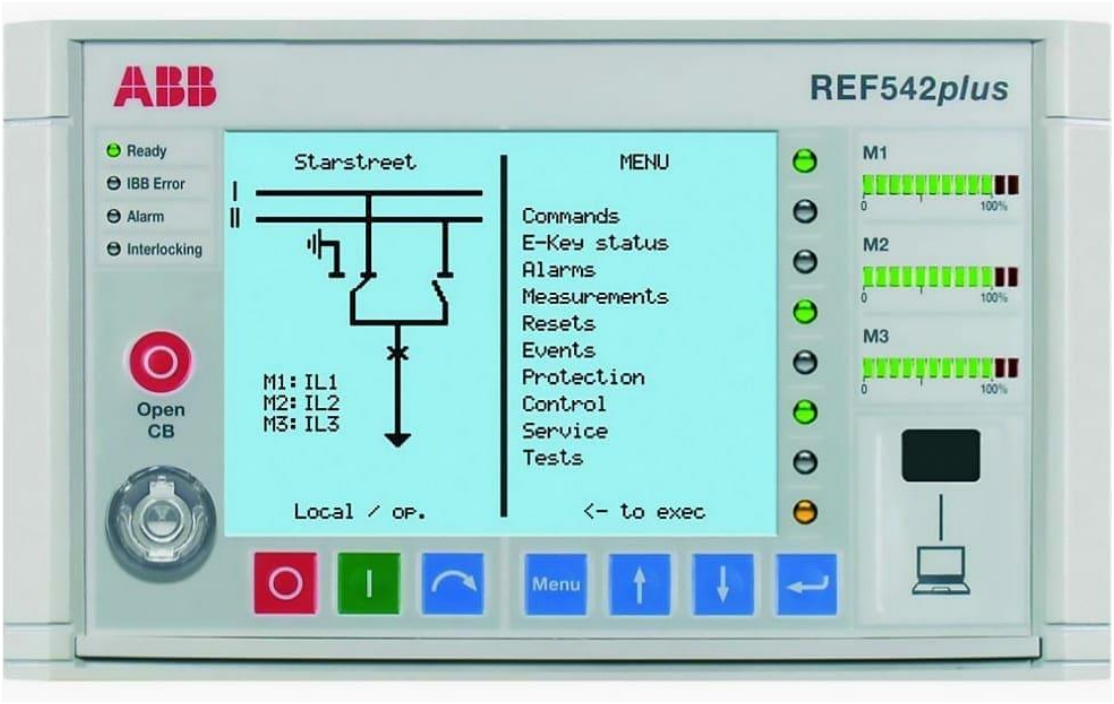
2. Remote Terminal Unit (RTU): είναι μια συσκευή ελέγχου που χρησιμοποιείται στα συστήματα SCADA για την παρακολούθηση και τον έλεγχο διαφόρων διεργασιών σε απομακρυσμένες τοποθεσίες. Το RTU συλλέγει δεδομένα από αισθητήρες και άλλες συσκευές στο πεδίο και μεταδίδει αυτά τα δεδομένα στο κεντρικό σύστημα ελέγχου για επεξεργασία και ανάλυση. Λαμβάνει επίσης εντολές ελέγχου από το κεντρικό σύστημα ελέγχου και τις στέλνει στις κατάλληλες συσκευές πεδίου για εκτέλεση [16]. Παίζει κρίσιμο ρόλο στη διασφάλιση της ασφαλούς και αποτελεσματικής λειτουργίας των συστημάτων SCADA.

[2] https://worktech.gr/plc/

Εικόνα 2.1-iii: Remote Terminal Unit. Πηγή: wikipedia.org[3]

3. Intelligent Electronic Device (IED): είναι μια συσκευή που χρησιμοποιείται σε συστήματα ισχύος για την προστασία, τον έλεγχο και την παρακολούθηση του εξοπλισμού ισχύος. Τα IED χρησιμοποιούνται συνήθως για την εκτέλεση σύνθετων λειτουργιών όπως η ανίχνευση σφαλμάτων, η απομόνωση και η αποκατάσταση, και είναι ικανά να επικοινωνούν με άλλες συσκευές στο σύστημα ισχύος μέσω διαφόρων πρωτοκόλλων όπως τα IEC 61850, DNP3 και Modbus [6].Τα IED είναι κρίσιμα εξαρτήματα στα σύγχρονα συστήματα ηλεκτρικής ενέργειας και διαδραματίζουν σημαντικό ρόλο στη διασφάλιση της ασφαλούς και αξιόπιστης λειτουργίας του ηλεκτρικού δικτύου.

[3] https://en.wikipedia.org/wiki/Remote_terminal_unit



Εικόνα 2.1-iv: Intelligent Electronic Device. Πηγή: electrical-engineering-portal.com[4]

2.1.2.2 Κεντρικό σύστημα ελέγχου

Το κεντρικό σύστημα ελέγχου είναι το νευρικό κέντρο ενός συστήματος SCADA όπου οι χρήστες παρακολουθούν και ελέγχουν τις βιομηχανικές διαδικασίες εξ αποστάσεως [5]. Αποτελείται συνήθως από μια αίθουσα ελέγχου εξοπλισμένη με μια σειρά προηγμένων εργαλείων υλικού και λογισμικού που έχουν σχεδιαστεί για να εξασφαλίζουν συνεχή παρακολούθηση και έλεγχο του συστήματος. Το κεντρικό σύστημα ελέγχου στελεχώνεται από εκπαιδευμένους χειριστές που είναι υπεύθυνοι για την παρακολούθηση της απόδοσης του συστήματος, τον εντοπισμό πιθανών προβλημάτων και τη λήψη διορθωτικών μέτρων για την αποφυγή διαταραχών στο σύστημα. Απαιτεί αξιόπιστη υποδομή επικοινωνίας για την εξασφάλιση παρακολούθησης και ελέγχου σε πραγματικό χρόνο των βιομηχανικών διαδικασιών[28]. Τα συστήματα επικοινωνίας, όπως τα τοπικά δίκτυα (LAN) και τα δίκτυα ευρείας περιοχής (WAN), χρησιμοποιούνται για τη σύνδεση του κέντρου ελέγχου με τις συσκευές πεδίου, όπως οι RTUs (Remote Terminal Units), οι αισθητήρες, οι ενεργοποιητές και άλλα μέσα συλλογής ή εκτέλεσης εντολών. Οι RTUs

[4] https://electrical-engineering-portal.com/ied-intelligent-electronic-device-advanced-functions

λειτουργούν ως ενδιάμεσοι κόμβοι, μεταφέροντας δεδομένα από τον εξοπλισμό πεδίου στο κεντρικό σύστημα και αντίστροφα. Αυτό επιτρέπει στους χειριστές να παρακολουθούν και να ελέγχουν τις βιομηχανικές διεργασίες από μια κεντρική τοποθεσία, μειώνοντας την ανάγκη για επιτόπιες επιθεωρήσεις και χειρωνακτικές παρεμβάσεις.

Η ασφάλεια είναι μια κρίσιμη ανησυχία για το κεντρικό σύστημα ελέγχου στα συστήματα SCADA. Το κεντρικό σύστημα ελέγχου είναι υπεύθυνο για την προστασία του συστήματος από τη μη εξουσιοδοτημένη πρόσβαση, κυβερνοεπιθέσεις και άλλες απειλές που μπορούν να προκαλέσουν διακοπές στις βιομηχανικές διαδικασίες. Το κεντρικό σύστημα ελέγχου πρέπει να εφαρμόζει προηγμένα μέτρα ασφαλείας, όπως firewall, συστήματα ανίχνευσης εισβολών και τεχνολογίες κρυπτογράφησης, για την προστασία του συστήματος από απειλές ασφαλείας[6].

Οι τρεις χαρακτηριστικές συσκευές του κεντρικού συστήματος ελέγχου είναι:

1. Master Terminal Unit (MTU): είναι ένα κρίσιμο στοιχείο στα συστήματα SCADA που συλλέγει και επεξεργάζεται δεδομένα σε πραγματικό χρόνο από τις συσκευές πεδίου, μέσω διαφόρων καναλιών επικοινωνίας, συμπεριλαμβανομένων σειριακών, Ethernet και ασύρματων. Τα MTU είναι υπεύθυνα για την παρακολούθηση και τον έλεγχο των βιομηχανικών διεργασιών, καθώς και για την παροχή απομακρυσμένης πρόσβασης και διαγνωστικών δυνατοτήτων στους χειριστές στα κέντρα ελέγχου. Ακόμη, έχουν την δυνατότητα να προ επεξεργάζονται τα δεδομένα πριν τα στείλουν στον Historian (εξηγείται παρακάτω)[6]. Τα MTU έχουν σχεδιαστεί για να είναι αξιόπιστα, επεκτάσιμα και ασφαλή, με πλεονάζοντα τροφοδοτικά, επεξεργαστές και συνδέσεις επικοινωνίας για να διασφαλίζουν τη συνεχή λειτουργία ακόμη και σε περίπτωση βλάβης. Μπορούν να αποθηκεύουν και να αναλύουν μεγάλες ποσότητες δεδομένων που συλλέγονται από συσκευές πεδίου, όπως μετρήσεις αισθητήρων, συναγερμοί και συμβάντα, χρησιμοποιώντας προηγμένους αλγόριθμους και τεχνικές επεξεργασίας δεδομένων. Τέλος, τα MTU είναι κρίσιμοι στόχοι για κυβερνοεπιθέσεις επειδή είναι οι κύριες πύλες μεταξύ του κεντρικού συστήματος ελέγχου και των συσκευών πεδίου [21].
2. Human-Machine Interface (HMI): είναι η γραφική διεπαφή χρήστη που χρησιμοποιείται για την παρακολούθηση και τον έλεγχο της βιομηχανικής

διαδικασίας που εποπτεύεται. Είναι το μέσο με το οποίο οι χειριστές μπορούν να αλληλοεπιδράσουν με το κεντρικό σύστημα ελέγχου, συμπεριλαμβανομένων των PLC, των RTU και άλλων συσκευών πεδίου. Το HMI παρουσιάζει δεδομένα από τη διαδικασία σε πραγματικό χρόνο και παρέχει επιλογές ελέγχου στον χειριστή. Αποτελείται συνήθως από έναν υπολογιστή με γραφική οθόνη και συσκευές εισόδου, όπως ένα πληκτρολόγιο και ένα ποντίκι [12]. Η γραφική οθόνη εμφανίζει δεδομένα από τη διαδικασία σε διάφορες μορφές, όπως γραφήματα και πίνακες. Το HMI μπορεί επίσης να παρέχει συναγερμούς και ειδοποιήσεις στον χειριστή, ενημερώνοντάς τον για τυχόν προβλήματα με τη διαδικασία ή τον εξοπλισμό. Οι χειριστές μπορούν να αλληλοεπιδράσουν με το HMI για να προσαρμόσουν τα σημεία ρύθμισης, να ξεκινήσουν ενέργειες και να τροποποιήσουν τη συμπεριφορά του κεντρικού συστήματος ελέγχου. Ένα αποτελεσματικό HMI θα πρέπει να παρέχει στους χειριστές σαφείς και συνοπτικές πληροφορίες, να είναι διαισθητικό στη χρήση και να ελαχιστοποιεί τον κίνδυνο σφαλμάτων χειριστή. Ένα καλά σχεδιασμένο HMI μπορεί να βοηθήσει στη βελτίωση της αποδοτικότητας της βιομηχανικής διαδικασίας, στη μείωση του χρόνου διακοπής λειτουργίας και στη βελτίωση της συνολικής απόδοσης του συστήματος [6].

3. Historian: είναι ένα κρίσιμο στοιχείο ενός συστήματος SCADA που χρησιμεύει στην αποθήκευση όλων των λειτουργικών δεδομένων που συλλέγονται από διάφορες συσκευές και αισθητήρες του συστήματος. Επιτρέπει τη μακροπρόθεσμη αποθήκευση και ανάκτηση ιστορικών δεδομένων για ανάλυση και λήψη αποφάσεων [1]. Το Historian παίζει βασικό ρόλο στη διατήρηση της ακεραιότητας και της ακρίβειας των δεδομένων εξαλείφοντας πλεονασμούς και διατηρώντας τη συνέπεια των πληροφοριών σε όλο το σύστημα. Μπορεί να συλλέγει, αποθηκεύει και να διαχειρίζεται δεδομένα με δομημένο και οργανωμένο τρόπο που επιτρέπει την εύκολη πρόσβαση και ανάκτηση πληροφοριών. Ακόμη είναι ικανό να χειριστεί μεγάλους όγκους δεδομένων από διάφορες πηγές και παρέχει τη δυνατότητα αναζήτησης, φιλτραρίσματος και ανάκτησης δεδομένων με βάση διάφορες παραμέτρους [24]. Μπορεί επίσης να δημιουργήσει αναφορές και απεικονίσεις για να βοηθήσει τους χειριστές και τους αναλυτές να αποκτήσουν πληροφορίες για την απόδοση του συστήματος και να εντοπίσουν τάσεις και ανωμαλίες. Τα δεδομένα που είναι αποθηκευμένα στο Historian μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, όπως

παρακολούθηση απόδοσης, προγνωστική συντήρηση, ανίχνευση σφαλμάτων και βελτιστοποίηση του συστήματος. Το Historian παρέχει μια αξιόπιστη και ασφαλή λύση αποθήκευσης δεδομένων που διασφαλίζει την ακεραιότητα και τη συνέχεια των δεδομένων, ακόμη και σε περίπτωση αστοχιών ή καταστροφών του συστήματος.

2.1.2.3 Επικοινωνία δικτύων

Τα συστήματα SCADA βασίζονται σε μεγάλο βαθμό στην επικοινωνία δικτύου για τη μετάδοση δεδομένων από τις συσκευές πεδίου στο κεντρικό σύστημα ελέγχου. Αυτό το δίκτυο επικοινωνίας αποτελείται συνήθως από διάφορες συσκευές όπως switches, routers, firewalls, and gateways. Τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στα δίκτυα SCADA ποικίλλουν ανάλογα με τις συγκεκριμένες συσκευές και τις εφαρμογές που εμπλέκονται, αλλά τα πιο συχνά χρησιμοποιούμενα πρωτόκολλα περιλαμβάνουν τα Modbus, DNP3 και Profibus [5]. Εκτός από τα ενσύρματα δίκτυα, τα συστήματα SCADA μπορούν επίσης να χρησιμοποιούν τεχνολογίες ασύρματης επικοινωνίας όπως Wi-Fi, cellular ή satellite. Η ασύρματη επικοινωνία μπορεί να χρησιμοποιηθεί για την επέκταση της εμβέλειας των συστημάτων SCADA σε απομακρυσμένες ή δυσπρόσιτες τοποθεσίες όπου τα ενσύρματα δίκτυα δεν είναι εφικτά [25]. Ωστόσο, τα ασύρματα δίκτυα μπορούν επίσης να εισάγουν πρόσθετους κινδύνους για την ασφάλεια και απαιτούν προσεκτικό σχεδιασμό και εφαρμογή για να διασφαλιστεί η αξιοπιστία και η ασφάλειά τους.

2.2 Ο Ρόλος των Συστημάτων SCADA στις Κρίσιμες Υποδομές

Τα συστήματα SCADA είναι συστήματα εποπτικού ελέγχου που όταν εφαρμόζονται στη βιομηχανία ενέργειας, μπορούν να βοηθήσουν στην εξοικονόμηση χρόνου και χρήματος, στη μείωση του κόστους λειτουργίας και στη βελτίωση της αποδοτικότητας [25]. Επιτρέπουν, επίσης, την παρακολούθηση σε πραγματικό χρόνο και την αυτοματοποίηση των έξυπνων δικτύων ηλεκτρικής ενέργειας, τα οποία αποτελούν πολλά υποσχόμενες λύσεις για την παροχή ηλεκτρικής ενέργειας στο μέλλον.

Τα SCADA ελέγχουν και παρακολουθούν σχεδόν όλες τις κρίσιμες υποδομές. Σύμφωνα με το Cybersecurity & Infrastructure Security Agency (CISA) υπάρχουν 16 κρίσιμες υποδομές. Αυτές περιλαμβάνουν την ενέργεια, τα απόβλητα καθώς και τα συστήματα ύδρευσης, τις τηλεπικοινωνίες, τις μεταφορές, τα χημικά φράγματα, τις υπηρεσίες έκτακτης ανάγκης, τις χρηματοπιστωτικές υπηρεσίες, τις εμπορικές εγκαταστάσεις, τις κυβερνητικές εγκαταστάσεις, τις χρηματοπιστωτικές υπηρεσίες, τις κρίσιμες εθνικές κατασκευές, και τους τομείς όπως είναι η άμυνα, τα τρόφιμα η γεωργία, και η υγεία [1].

Η αλληλεξάρτηση αυτών των κρίσιμων υποδομών εντείνει τους κινδύνους. Για παράδειγμα, μια επίθεση στον τομέα των τηλεπικοινωνιών μπορεί να έχει άμεσο αντίκτυπο στον τομέα της ενέργειας ή των μεταφορών. Στο πλαίσιο αυτό, τα συστήματα SCADA διαδραματίζουν κεντρικό ρόλο, καθώς παρέχουν δυνατότητες παρακολούθησης, ανάλυσης και λήψης αποφάσεων σε πραγματικό χρόνο. Για παράδειγμα, στις επιχειρήσεις κοινής ωφέλειας, τα SCADA προσφέρουν κρίσιμες πληροφορίες για την αποτελεσματική και ασφαλή διαχείριση της ενέργειας [3].

Καθώς οι κρίσιμες υποδομές εξαρτώνται ολοένα και περισσότερο από τεχνολογίες SCADA, η προστασία τους από σύγχρονες απειλές αποτελεί προτεραιότητα κυβερνοασφάλειας σε διεθνές επίπεδο [10].

2.3 Κυβερνοαπειλές και Τρωτά Σημεία στα συστήματα SCADA

2.3.1 Γενικές Απειλές και Προκλήσεις

Τα συστήματα SCADA διαδραματίζουν κρίσιμο ρόλο στη λειτουργία των σύγχρονων υποδομών, και επομένως η κυβερνοασφάλειά τους αποτελεί βασικό παράγοντα για την προστασία τους έναντι των κυβερνοαπειλών. Η αυξανόμενη διασύνδεση αυτών των συστημάτων με δίκτυα πληροφορικής και το διαδίκτυο έχει επιφέρει σημαντικά οφέλη στη λειτουργικότητα, αλλά ταυτόχρονα έχει τον κίνδυνο των κυβερνοεπιθέσεων. Η κατανόηση των απειλών που αντιμετωπίζουν τα SCADA, καθώς και η ανάλυση των

τρωτών σημείων τους, είναι θεμελιώδη στοιχεία για την ανάπτυξη αποτελεσματικών στρατηγικών άμυνας.

Η διασφάλιση των συστημάτων SCADA σε περιβάλλοντα κοινής ωφέλειας είναι δύσκολη λόγω των πολυάριθμων τρωτών σημείων που ενυπάρχουν στα δίκτυα επικοινωνίας, καθώς τα συστήματα SCADA γίνονται μεγαλύτερα, συνδέονται με άλλα δίκτυα, όπως το Διαδίκτυο. Η διασυνδεσιμότητα των συστημάτων SCADA στο δίκτυο ηλεκτρικής ενέργειας εκθέτει τα συστήματα SCADA σε ένα ευρύ φάσμα θεμάτων ασφάλειας επικοινωνιών [20].

Έτσι υπόκεινται σε νέους τύπους απειλών και επιθέσεων στον κυβερνοχώρο, όπως επιθέσεις man-in-the-middle, επιθέσεις άρνησης παροχής υπηρεσιών (DoS), επιθέσεις κοινωνικής μηχανικής και επιθέσεις εκ των έσω, εκθέτοντάς τα έτσι σε ένα ευρύ φάσμα ζητημάτων ασφάλειας επικοινωνίας. Οι στόχοι των επιτιθέμενων είναι να θέσουν σε κίνδυνο τα χαρακτηριστικά ασφαλείας του δικτύου, όπως η διαθεσιμότητα, η αυθεντικοποίηση, η εμπιστευτικότητα και η ακεραιότητα [10].

Ενα από τα πλέον πιθανά σενάρια επίθεσης είναι η υποκλοπή των γραμμών επικοινωνίας μεταξύ του διακομιστή SCADA και της RTU. Αυτό μπορεί να αντιμετωπιστεί με αντίμετρα, όπως και με συσκευές ασφαλείας για την κρυπτογράφηση και την αποκρυπτογράφηση των πληροφοριών [21]. Η πιστοποίηση πρόσβασης μεταξύ της RTU και του κύριου συστήματος είναι επίσης απαραίτητη, όπως και η χρήση έξυπνων καρτών, τειχών προστασίας και τα συστήματα ανίχνευσης εισβολών [3].

Οι προμηθευτές λογισμικού SCADA καλούνται να ενσωματώνουν ισχυρά χαρακτηριστικά ασφαλείας στα συστήματά τους ώστε να ανταποκρίνονται στις διαρκώς αυξανόμενες απειλές. Επιπλέον, πέρα από τις προκλήσεις ασφάλειας, η υλοποίηση και η συντήρηση ενός συστήματος SCADA είναι δαπανηρή και απαιτεί εξειδικευμένη εκπαίδευση προσωπικού, γεγονός που αυξάνει το συνολικό κόστος λειτουργίας [16].

2.3.2 Κατηγοριοποίηση Τρωτών Σημείων

Υπάρχουν πολλοί διαφορετικοί τύποι απειλών κατά καίριων υποδομών. Σύμφωνα με το [11], οι κυβερνοεπιθέσεις και οι σχετικές αδυναμίες (vulnerabilities) μπορούν να κατηγοριοποιηθούν ανάλογα με τον στόχο ως εξής:

1. Συστήματα SCADA (Hardware):
    - Φυσική πρόσβαση: επίθεση από έναν εισβολέα που αποκτά μη εξουσιοδοτημένη πρόσβαση.
    - Αλλαγή στις ρυθμίσεις: ένας επιτιθέμενος μπορεί να τροποποιήσει κρίσιμες τιμές κατωφλιού (thresholds) στο σύστημα, επηρεάζοντας σοβαρά τη λειτουργία τους.
    - Επίθεση τροποποίησης υλικολογισμικού (Firmware modification attack): η επίθεση περιλαμβάνει την τροποποίηση του υλικολογισμικού των συσκευών SCADA μέσω εισαγωγής κακόβουλου λογισμικού.
    - Ιός Stuxnet: ένα γνωστό παράδειγμα κυβερνοεπίθεσης που στοχεύει κρίσιμες υποδομές σε εργοστάσια ενέργειας, κρύβοντας τις κακόβουλες λειτουργίες του.
    - Επίθεση σε RTUs και PLCs: η εκμετάλλευση των RTUs και PLCs μπορεί να οδηγήσει σε αυτόματη εκτέλεση ανεπιθύμητων ελέγχων και ενεργειών.
2. Στο λογισμικό τους (Software):
    - Σχεδιασμός και υλοποίηση πηγαίου κώδικα (Source Code Design and Implementation): η αδυναμία αναφέρεται στον πηγαίο κώδικα του λογισμικού. Ένας κακός σχεδιασμός του μπορεί να περιέχει κενά ασφαλείας που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι.
    - Υπερχείλιση μνήμης (Buffer Overflow): η επίθεση εκμεταλλεύεται αδυναμίες στην διαχείριση μνήμης ενός προγράμματος. Όταν υπερφορτωθεί μια περιοχή μνήμης (buffer), μπορεί να παρακάμψει τις κρυφές τιμές και να εκτελέσει κακόβουλο κώδικα.
    - SQL Injection: αυτή η τεχνική εκμεταλλεύεται αδυναμίες στις βάσεις δεδομένων, όπου οι επιτιθέμενοι εισάγουν SQL εντολές σε πεδία εισόδου.
    - Cross site scripting: η επίθεση επιτρέπει στους κακόβουλους χρήστες να εισάγουν κακόβουλο κώδικα σε ιστοσελίδες, ο οποίος εκτελείται στον φυλλομετρητή (web browser) του χρήστη.

- Αποτελεσματική διαχείριση ενημερώσεων (Effective Patch Management Application): η έλλειψη τακτικών ενημερώσεων στα συστήματα SCADA μπορεί να τα καταστήσει ευάλωτα σε επιθέσεις.

3. Στο δίκτυο επικοινωνιών τους:
    - Μη απαραίτητες θύρες και υπηρεσίες (Unnecessary Ports and Services): οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις θύρες για να αποκτήσουν πρόσβαση στο δίκτυο.
    - Αδυναμίες καναλιών επικοινωνίας (Communication Channel Vulnerabilities): οι αδυναμίες αυτές αφορούν την ασφάλεια των καναλιών επικοινωνίας που χρησιμοποιούνται για την μετάδοση δεδομένων. Οι επιτιθέμενοι μπορούν να παρακολουθήσουν την ροή δεδομένων, αποκτώντας πρόσβαση σε ευαίσθητες πληροφορίες.
    - Αδυναμίες στα πρωτόκολλα επικοινωνιάς (Vulnerabilities of Communication Protocols): αυτές οι αδυναμίες σχετίζονται με τα πρωτόκολλα που καθορίζουν την επικοινωνία μεταξύ συσκευών. Επιθέσεις όπως DoS (Denial of Service) ή spoofing μπορεί να εκμεταλλευτούν αυτές τις αδυναμίες.

Τέλος, αξίζει να σημειωθεί μια ακόμη μορφή κυβερνοεπίθεσης, οι τεχνικές social engineer. Οι επιτιθέμενοι προσπαθούν μέσω email ή τηλεφώνου να αποσπάσουν κρίσιμες πληροφορίες, όπως κωδικούς ή αδυναμίες, για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα συστήματα.

Οι κυβερνοεπιθέσεις μπορεί να κλιμακωθούν μέσω διαφόρων φορέων όπως μέσω φυσικών δικτύων, απευθείας μέσω Διαδικτύου ή απομακρυσμένα με πρόσβαση μέσω ενός φορητού υπολογιστή ή κινητού τηλεφώνου [21]. Ακόμη, η ραγδαία εξέλιξη της τεχνολογίας έχει οδηγήσει σε πιο εξελιγμένες μεθόδους επίθεσης στα συστήματα SCADA που χρησιμοποιούν κινητές συσκευές όπως tablets και κινητά τηλέφωνα [24]. Επομένως, υπάρχουν πολλές απειλές στον κυβερνοχώρο κατά των συστημάτων SCADA με εξελιγμένες επιθέσεις κακόβουλου λογισμικού, ενώ συνεχώς ανακαλύπτονται νέοι τρόποι επιθέσεων κυρίων με ψηφιακά μέσα.

2.4 Ψηφιακή Εγκληματολογική διερεύνηση Κυβερνοεπιθέσεων στα συστήματα SCADA

2.4.1 Σκοπός και Σημασία της Ψηφιακής Εγκληματολογικής Διερεύνησης

Η ψηφιακή εγκληματολογική διερεύνηση (digital forensics) για την Κυβερνοασφάλεια είναι μια συνεχής διαδικασία απόκτησης, εξέτασης, ανάλυσης και αναφοράς των αποδεικτικών στοιχείων. Η ψηφιακή εγκληματολογική διερεύνηση για την Κυβερνοασφάλεια είναι ένας από τους βασικούς κλάδους της κυβερνοάμυνας και συνδέεται άμεσα με την λογοδοσία ιδιαίτερα όταν υπάρχει παραβίαση ασφαλείας [6]. Είναι σημαντικό να διεξαχθεί σωστά η έρευνα μετά το συμβάν για την αποφυγή απώλειας υπό διερεύνηση δεδομένων (αποδεικτικών στοιχείων). Επιπλέον, η σωστή έρευνα βοηθά στην κατανόηση των αιτιών και των αποτελεσμάτων των επιθέσεων εισβολής. Πρόσφατες επιθέσεις κατά των συστημάτων SCADA καταδεικνύουν ότι οι σχετικές έρευνες καθίστανται απαραίτητες και πρέπει να πραγματοποιηθούν για την βελτιωμένη άμυνα στον κυβερνοχώρο στα συστήματα SCADA [8]. Στο πλαίσιο της ψηφιακής εγκληματολογικής διερεύνησης, ο υπεύθυνος ερευνητής επικεντρώνεται κυρίως στη συλλογή των αποδεικτικών στοιχείων από μια συσκευή ή ένα δίκτυο και ο κύριος στόχος του είναι η διερεύνηση του περιστατικού, η αξιολόγηση της επίδρασής του στο σύστημα και η ταυτοποίηση του υπευθύνου για την κυβερνοεπίθεση.

Είναι κρίσιμο μετά από ένα περιστατικό ασφάλειας να αρχίσει άμεσα, το συντομότερο δυνατό, η διερεύνηση της απειλής/επίθεσης για να αποτραπεί η απώλεια αποδεικτικών στοιχείων που καταδεικνύουν κακόβουλη ενέργεια. Η έρευνα θα πρέπει, επίσης, να ακολουθήσει ορισμένη στρατηγική, η οποία θα έχει προβλεφθεί για παρόμοια περιστατικά. Για παράδειγμα, η έρευνα θα πρέπει να εντοπίζει πώς πραγματοποιήθηκε η επίθεση, ποιοι ήταν οι δράστες της και πως μπορεί να προστατευτεί το σύστημα SCADA από μελλοντικές επιθέσεις. Συνεπώς, η διερεύνηση αποδεικνύεται ιδιαίτερα σημαντική και πρέπει να πραγματοποιείται μετά από κάθε περιστατικό (incident), είτε στον ψηφιακό τομέα είτε σε κρίσιμες φυσικές υποδομές και εγκαταστάσεις [19]. Σύμφωνα με [15], μια σωστή στρατηγική θα είναι σε θέση να βοηθήσει μια έρευνα αν μπορεί να απαντήσει στις παρακάτω ερωτήσεις:

- Διαπιστώθηκε ότι ο ιός μπορούσε να κλέψει ευαίσθητες πληροφορίες και αν ναι τι πληροφορίες ήταν αυτές;
- Αν διαπιστώθηκε ότι ο συγκεκριμένος ιός προκάλεσε τελικά δυσλειτουργία, ποια ήταν η αιτία και είναι το σύστημα ακόμα σε κίνδυνο;
- Σε ποια έκταση έχει επηρεάσει ο ιός το συγκεκριμένο σύστημα;

Επομένως ένας ερευνητής θα πρέπει να γνωρίζει τις τυπικές μεθόδους επίθεσης ιδιαίτερα στα συστήματα SCADA και τις αυξανόμενες απειλές νέων επιθέσεων λόγω της μεγάλης τεχνολογικής ανάπτυξης και των συνεχώς εξελισσόμενων ψηφιακών τεχνολογιών [16]. Η διεξαγωγή τέτοιων ερευνών παρουσιάζει πλέον προκλήσεις και οι ερευνητές θα πρέπει συνεχώς να αναπτύσσουν στρατηγικές και εργαλεία που θα αντιμετωπίζουν αποτελεσματικά κυβερνοαπειλές και επιθέσεις. Παράλληλα, ιδιαίτερη έμφαση πρέπει να δίνεται στην πρόληψη, έτσι ώστε να μπορούν οι κακόβουλες ενέργειες να εντοπίζονται και να αποτρέπονται εγκαίρως.

Πέρα από την ανάλυση και πρόληψη μελλοντικών περιστατικών, τα ευρήματα της ψηφιακής εγκληματολογικής διερεύνησης έχουν καθοριστικό ρόλο και στην τεκμηρίωση για νομικούς σκοπούς. Τα συλλεγμένα ψηφιακά ίχνη και τα αρχεία καταγραφής (logs) μπορούν να αξιοποιηθούν ως αποδεικτικά στοιχεία σε εσωτερικούς ελέγχους ή νομικές διαδικασίες, εφόσον τηρούνται τα πρότυπα ακεραιότητας και αλυσίδας φύλαξης στοιχείων (chain of custody). Επιπλέον, η σωστή τεκμηρίωση αποτελεί βασική απαίτηση κανονιστικών πλαισίων όπως η οδηγία NIS2[5] για την ασφάλεια δικτύων και πληροφοριακών συστημάτων στην Ε.Ε., αλλά και ο κανονισμός GDPR[6], ειδικά σε περιπτώσεις παραβίασης προσωπικών δεδομένων. Η δυνατότητα απόδειξης της αντίδρασης σε ένα περιστατικό (πότε συνέβη, πώς αντιμετωπίστηκε, ποια μέτρα εφαρμόστηκαν) μπορεί να επηρεάσει σημαντικά τόσο τη συμμόρφωση όσο και την ευθύνη ενός οργανισμού.

[5] https://digital-strategy.ec.europa.eu/el/policies/nis2-directive

[6] https://gdpr.eu/what-is-gdpr/

2.4.2 Τυπικά στάδια Ψηφιακής Εγκληματολογικής διερεύνησης

Η έρευνα μιας απειλής ή κυβερνοεπίθεσης είναι κρίσιμη καθώς συμβάλλει στην ανάλυση των γεγονότων μετά από ένα περιστατικό και επιτρέπει την ανάπτυξη αποδοτικών μέτρων αντίδρασης [6]. Ο σκοπός της ψηφιακής εγκληματολογικής διερεύνησης είναι να διασφαλίσει ότι η συλλογή στοιχείων για τον εντοπισμό μια κυβερνοεπίθεσης γίνεται με επιστημονικά τεκμηριωμένο και νόμιμο τρόπο, προκειμένου να υποστηριχθεί η εγκυρότητα των ευρημάτων. Χρειάζονται βέβαια να γίνουν πολλά βήματα για τη διεξαγωγή μιας ψηφιακής εγκληματολογικής διερεύνησης εντοπισμού κακόβουλου λογισμικού όπως είναι η διατήρηση, ταυτοποίηση, εξαγωγή και τεκμηρίωση των ψηφιακών αποδεικτικών στοιχείων. Σύμφωνα με τους Radvanovsky και Brodsky τα ερευνητικά στάδια είναι τα ακόλουθα:

Βήμα 1: Εξέταση. Κατά το πρώτο βήμα, είναι απαραίτητο να εντοπιστούν όλα τα πιθανά σημεία από όπου μπορεί να συλλεχθούν στοιχεία, όπως οι συσκευές δικτύου ή οι συσκευές του συστήματος. Εκτός από αυτές τις πηγές θα πρέπει να διεξαχθεί έρευνα και να εξεταστούν και άλλα συστήματα που έχουν σχέση με το σύστημα SCADA, όπως τερματικά πρόσβασης (terminals), διακομιστές και δρομολογητές (routers).

Βήμα 2: Αναγνώριση. Σε αυτό το βήμα γίνεται η αναγνώριση των συστημάτων που θα διερευνηθούν. Είναι σημαντικό να σημειωθεί ότι ένα σύστημα μπορεί να χρησιμοποιεί πολλαπλά λειτουργικά συστήματα, όπως κάποια έκδοση Linux, ενώ πολλά SCADA συστήματα λειτουργούν με θυγατρικά συστήματα πάνω από ένα κύριο λειτουργικό. Αυτό αυξάνει την πολυπλοκότητα της διαχείρισης και της ασφάλειας. Επομένως, η αναγνώριση αυτών των πολλαπλών λειτουργικών βοηθά να έχουμε πλήρη εικόνα του συστήματος.

Βήμα 3: Συλλογή. Σε αυτό το βήμα συλλέγονται πιθανά αποδεικτικά στοιχεία από την μνήμη του συστήματος. Είναι κρίσιμο να συγκεντρωθούν πρώτα οι ευμετάβλητες πληροφορίες, προκειμένου να αποτραπεί η απώλεια δεδομένων.

Βήμα 4: Τεκμηρίωση. Στο τελευταίο βήμα είναι κρίσιμο να διατηρηθεί η ακριβής τεκμηρίωση της έρευνας, προκειμένου να διασφαλιστεί η εγκυρότητα και η αξιοπιστία των αποδεικτικών στοιχείων. Τα αποδεικτικά στοιχεία που συλλέγονται πρέπει να διατηρούνται σε αρχεία που θα περιλαμβάνουν και τον χρόνο κατά τον οποίο συγκεντρώθηκαν τα στοιχεία αυτά. Τέλος, κρίνεται απαραίτητο η αναφορά ολόκληρης της ψηφιακής ερευνητικής διαδικασίας να εκπονηθεί λεπτομερώς. Το τελευταίο στάδιο

είναι η συλλογή και ενοποίηση όλων των πληροφοριών και η αποθήκευση τους σε ασφαλή και απόλυτα ελεγχόμενη τοποθεσία.

Στο ίδιο άρθρο [24], ο Wu προτείνει ένα νέο μοντέλο για την ψηφιακή εγκληματολογική διερεύνηση. Σκοπός της νέας αυτής πρότασης για ένα πιο εξελιγμένο μοντέλο είναι ότι οι υπάρχουσες διαδικασίες στερούνται λεπτομέρειας σχετικά με τη διενέργεια πλήρους έρευνας σε ένα σύστημα SCADA για την αντιμετώπιση ενός περιστατικού (incident) ιδιαίτερα όταν αυτό γίνεται στον κυβερνοχώρο. Αυτό το εξελιγμένο μοντέλο έχει πρόσθετες φάσεις όπως φαίνονται παρακάτω:

- Φάση 1- Ταυτοποίηση και Προετοιμασία
- Φάση 2- Προσδιορισμός πηγών δεδομένων
- Φάση 3- Διατήρηση, Προτεραιότητα και Συλλογή
- Φάση 4- Εξέταση
- Φάση 5- Ανάλυση
- Φάση 6- Αναφορά Παρουσίαση
- Φάση 7 Ανασκόπηση αποτελεσμάτων

Αναλυτικότερα:

Φάση 1- Ταυτοποίηση και προετοιμασία: Αυτή η φάση λαμβάνει χώρα πριν από την έρευνα, με στόχο την κατανόηση της αρχιτεκτονικής των συστημάτων SCADA, του δικτύου και πιθανώς την κατανόηση του είδους του περιστατικού που έχει συμβεί. Θα πρέπει να αναπτυχθεί μια κατάλληλη στρατηγική λαμβάνοντας υπόψη τα συστήματα, τον τύπο του περιστατικού και τους χρονικούς περιορισμούς, συμπεριλαμβανομένων των απαιτήσεων για τη λειτουργία των συστημάτων SCADA 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Αυτή είναι η συλλογή τεκμηρίωσης με τη συλλογή πληροφοριών από διάφορους πόρους και μέρη, συμπεριλαμβανομένων προμηθευτών, λογισμικού, παροχών υλικού και εργολάβων.

Φάση 2- Προσδιορισμός πηγών δεδομένων Απαιτείται τεκμηρίωση από τη φάση 2 έως τη φάση 7, επομένως στο τέλος της έρευνας μπορεί να συνταχθεί μια έκθεση για την παροχή συμπεράσματος των πορισμάτων από την έρευνα και την απόδειξη ότι η αλυσίδα των αποδεικτικών στοιχείων έχει τηρηθεί. Επίσης, ο προσδιορισμός του σημείου εισόδου περιλαμβάνει την εξέταση πιθανών σημείων εισόδου ή την πιθανή χρήση εξωτερικών συσκευών για την πρόσβαση στο σύστημα SCADA. Αυτά τα σημεία εισόδου μπορεί να περιλαμβάνουν μικρές κινητές συσκευές, ασύρματες συνδέσεις ή πρόσβασης μέσω DoS. Μια επίθεση μπορεί να στοχεύει σε

έναν υπολογιστή που εκτελεί μια μη ασφαλή εφαρμογή ή μια επίθεση σε μια κάμερα web που παρακολουθεί μια απομακρυσμένη συσκευή σε ένα δίκτυο SCADA. Αυτή είναι η φάση που εντοπίζονται πηγές δεδομένων, ανάλογα με τον τύπο του περιστατικού, οι οποίες μπορεί να έχουν αλληλοεπιδράσει με το συμβάν και να περιέχουν πιθανά αποδεικτικά δεδομένα. Σε αυτό το στάδιο, η χαρτογράφηση των λειτουργικών συστημάτων και συσκευών SCADA στο δίκτυο χρησιμοποιείται για την προετοιμασία μιας εργαλειοθήκης. δηλαδή συσκευές υλικού και λογισμικού που μπορεί να απαιτούνται για την αντιμετώπιση αυτού του συγκεκριμένου περιστατικού. Η ανάπτυξη ενός σχεδίου είναι ένα ζωτικό σημείο της έρευνας γιατί μπορεί να είναι πολλαπλές και διαφορετικές οι πηγές των δεδομένων. Το σχέδιο θα πρέπει να περιλαμβάνει την ιεράρχηση των πηγών δεδομένων, καθορίζοντας την σειρά με την οποία πρέπει να ληφθούν.

Φάση 3 - Προτεραιότητα, διατήρηση και συλλογή. Ο λόγος για την ιεράρχηση και τη διατήρηση των ασταθών δεδομένων είναι ότι, σε ένα σύστημα SCADA, μεγάλες ποσότητες δεδομένων διεργασίας συνδυάζονται με παρόμοιο τρόπο με τον τρόπο με τον οποίο τα δεδομένα αντικαθίστανται ή παραβιάζονται. Ως εκ τούτου, θα πρέπει να ληφθούν μέτρα για τη διατήρηση των σημαντικών δεδομένων και την ιεράρχηση των τρόπων συλλογής δεδομένων.

Φάση 4- Εξέταση. Αυτό το στάδιο περιλαμβάνει την εξέταση των αποδεικτικών στοιχείων που συλλέχθηκαν από ειδικευμένο ερευνητή. Αυτό το μέρος της διαδικασίας είναι πολύ σημαντικό επειδή παρέχει απαντήσεις σε ερωτήματα που τέθηκαν πριν από την έρευνα. Τα δεδομένα που συλλέγονται από ένα σύστημα SCADA συνήθως είναι τεράστιοι όγκοι αρχείων, επομένως αυτό είναι το μέρος της διάσπασης των αποδεικτικών στοιχείων σε διαχειρίσιμα φορτία για περαιτέρω ανάλυση. Θα πρέπει να προηγηθεί πρώτα ένα ξεκαθάρισμα όπως είναι το φιλτράρισμα, η αφαίρεση γνωστών ή μη χρήσιμων αρχείων, η αντιστοίχιση προτύπων, η αναζήτηση μέσω γνωστών τιμών κατακερματισμού και οι αναζητήσεις λέξεων-κλειδιών με βάση τις πληροφορίες που έχουν συλλεχθεί πριν από το συμβάν. Αυτή είναι η φάση που από την μία γίνεται ανάκτηση των δεδομένων και από την άλλη γίνεται προσπάθεια για τον εντοπισμό συστημάτων που έχουν παραβιαστεί ή τυχόν τροποποιηθεί. Είναι κατά τη διάρκεια αυτής της φάσης όπου ένας ερευνητής μπορεί να ανακαλύψει «παγίδες» ή συστήματα που ενδέχεται να συνδέονται με άλλες κακόβουλες διαδικασίες και ίσως χρειαστεί περαιτέρω συλλογή στοιχείων από ίδιες ή διαφορετικές πηγές δεδομένων.

Φάση 5- Ανάλυση. Αυτή είναι η φάση εύρεσης σχέσεων μεταξύ των ανακτηθέντων ερευνητικών δεδομένων σε συνδυασμό με τα αποδεικτικά στοιχεία που θα επιτρέψουν να αναπτυχθεί ένα χρονοδιάγραμμα αρχικά του συγκεκριμένου περιστατικού. Αυτό στην συνέχεια, καθιστά δυνατή την ανακατασκευή του συμβάντος σε ένα δοκιμαστικό περιβάλλον, για να βοηθήσει να δοθούν απαντήσεις σε ερωτήματα που προέκυψαν στο πλαίσιο της έρευνας που έγινε.

Φάση 6- Αναφορά και Παρουσίαση. Μετά τη φάση εξέτασης και ανάλυσης τα αποτελέσματα θα πρέπει να συγκεντρωθούν και να γίνει μια αναφορά η οποία θα πρέπει να παρουσιασθεί στους άμεσα ενδιαφερόμενους αρχικά και στην συνέχεια να διατηρηθεί ως ερευνητικό αρχείο αλλά και για στατιστικούς λόγους. Η αναφορά αυτή θα πρέπει να περιλαμβάνει οποιαδήποτε συμπεράσματα προέκυψαν από την έρευνα που έγινε, τις διάφορες φάσεις ανάλυσης και τις σχετικές απαντήσεις σε τυχόν ερωτήσεις που αφορούν το συμβάν.

Φάση 7- Εξέταση αποτελεσμάτων. Το τελικό στάδιο είναι η ανασκόπηση των αποτελεσμάτων από τις φάσεις της εξέτασης και ανάλυσης. Μια τέτοια έρευνα μπορεί να μην απαντήσει σε όλες τις ερωτήσεις που προκύπτουν κατά την διάρκειά της. Εάν τα αντικείμενα και στοιχεία που διερευνώνται δημιουργούν περισσότερες από μια εξηγήσεις, τότε πρέπει ο ερευνητής είτε να αποδείξει είτε να απορρίψει αυτές τις εξηγήσεις. Μία έκθεση που προσκομίζεται στους ενδιαφερόμενους αλλά και ακόμα σε δημόσια αρχή ή δικαστήριο ως αποδεικτικό υλικό, θα πρέπει να έχει λεπτομερή περιγραφή όλων των φάσεων έρευνας, και πιθανώς αποδεικτικά αντίγραφα των δεδομένων που συλλέχθηκαν. Για παράδειγμα, μία έκθεση που παρουσιάζεται από έναν μηχανικό δικτύου, θα απαιτούσε μια λεπτομερή αναφορά κυκλοφορίας δικτύου και επιπλέον λεπτομέρειες σχετικά με τα προσδιοριζόμενα πιθανά τρωτά σημεία στο σύστημα που απαιτούν προσοχή. Όπου δεν έχει συναχθεί συμπέρασμα κατά τη διάρκεια της αρχικής έρευνας πιθανόν θα πρέπει να συγκεντρωθούν περισσότερα στοιχεία και το συγκεκριμένο σύστημα SCADA θα πρέπει να διορθωθεί για να αποφευχθούν άλλες επιθέσεις στο μέλλον.

2.4.3 Κριτήρια και μεθοδολογίες ταξινόμησης απειλών στην κυβερνοασφάλεια

Η κατανόηση των τεχνικών ευπαθειών που περιεγράφηκαν παραπάνω αποτελεί τη βάση για την επόμενη φάση: την αξιολόγηση και κατηγοριοποίηση των απειλών με βάση ποιοτικά και ποσοτικά κριτήρια, ώστε να σχεδιαστούν αποτελεσματικές στρατηγικές άμυνας. Η ορθή διερεύνηση κυβερνοεπιθέσεων απαιτεί όχι μόνο την τεχνική ανάλυση αλλά και την αξιολόγηση και κατηγοριοποίηση των απειλών. Η παρούσα ενότητα παρουσιάζει τα βασικά κριτήρια και μεθοδολογίες ταξινόμησης που αξιοποιούνται στο πλαίσιο της ψηφιακής διερεύνησης SCADA περιστατικών.

Η ταξινόμηση των κυβερνοαπειλών αποτελεί κρίσιμο βήμα στην ανάλυση και αντιμετώπισή τους, καθώς επιτρέπει την ομαδοποίησή τους με βάση διάφορες διαστάσεις, όπως η προέλευση, η μορφή, η σοβαρότητα και η πιθανότητα εκδήλωσης. Η κατηγοριοποίηση αυτή βοηθά τόσο στη διαχείριση των κινδύνων όσο και στον σχεδιασμό κατάλληλων μέτρων προστασίας και αντίδρασης.

Ωστόσο, η αποτελεσματικότητα μιας τέτοιας ταξινόμησης δεν εξαρτάται μόνο από τα χαρακτηριστικά των ίδιων των απειλών, αλλά και από το κατά πόσο το πλαίσιο ταξινόμησης που χρησιμοποιείται είναι σαφές, αξιόπιστο και επεκτάσιμο. Συνεπώς, είναι εξίσου σημαντικό να αξιολογούνται και οι μεθοδολογίες που χρησιμοποιούνται για την οργάνωση και εφαρμογή της ταξινόμησης, με βάση ποιοτικά κριτήρια.

Συνεπώς, διακρίνουμε δύο επίπεδα κριτηρίων:

1. **Κριτήρια ταξινόμησης κυβερνοαπειλών**, τα οποία χρησιμοποιούνται για την ομαδοποίηση και κατηγοριοποίηση των απειλών με βάση συγκεκριμένες ιδιότητες.
2. **Κριτήρια αξιολόγησης ενός πλαισίου ταξινόμησης απειλών**, τα οποία καθορίζουν τις προϋποθέσεις που πρέπει να πληροί μια μεθοδολογία ταξινόμησης ώστε να είναι αξιόπιστη, σαφής και εφαρμόσιμη.

Οι κυριότερες παράμετροι που χρησιμοποιούνται για την περιγραφή και την ταξινόμηση των απειλών είναι:

1. Πηγή της απειλής:
   - Εσωτερικές απειλές (π.χ. εργαζόμενοι ή συνεργάτες).

- Εξωτερικές απειλές (π.χ. hackers, κρατικοί φορείς, εγκληματίες του κυβερνοχώρου).

2. Μορφή επίθεσης:
   - Malware (κακόβουλο λογισμικό).
   - Phishing (ηλεκτρονική απάτη).
   - Denial of Service (DDoS).
   - Εισβολές στο δίκτυο ή υποκλοπή δεδομένων.
   - Απειλές μέσω κοινωνικής μηχανικής.
3. Αντίκτυπος (impact):
   - Πολύ Υψηλός: Κίνδυνος για κρίσιμα συστήματα ή υποδομές.
   - Υψηλός: Σημαντική ζημιά σε συστήματα ή δεδομένα.
   - Μεσαίος: Σοβαρό πλήγμα σε κάποια συστήματα, αλλά χωρίς εκτεταμένη ζημιά.
   - Χαμηλός: Περιορισμένος αντίκτυπος ή δυνατότητα ανάκαμψης.
4. Πιθανότητα εκδήλωσης (likelihood):
   - Υψηλή: Είναι πολύ πιθανό να συμβεί η απειλή.
   - Μέτρια: Υπάρχει κάποια πιθανότητα.
   - Χαμηλή: Ελάχιστη πιθανότητα να συμβεί η απειλή.
5. Απαιτούμενοι πόροι για την επίθεση:
   - Χαμηλή: Οποιοσδήποτε κακόβουλος χρήστης μπορεί να επιτεθεί.
   - Μεσαία: Απαιτούνται κάποια τεχνικά μέσα ή ειδικές γνώσεις.
   - Υψηλή: Υποθέτει εξειδικευμένο προσωπικό ή μεγάλους πόρους για να συμβεί.
6. Διάρκεια εκτέλεσης:
   - Άμεση ή γρήγορη εκτέλεση της επίθεσης.
   - Αργή, αλλά με παρατεταμένη παρουσία και αντίκτυπο.
7. Εκμετάλλευση τρωτών σημείων (vulnerability):
   - Τρωτό σημείο του συστήματος που μπορεί να εκμεταλλευτεί η απειλή.
   - Χρησιμοποιούνται αδυναμίες στον σχεδιασμό ή στην υλοποίηση του συστήματος.

Για να είναι ένα πλαίσιο ταξινόμησης αποτελεσματικό, πρέπει να πληροί συγκεκριμένα ποιοτικά χαρακτηριστικά. Σύμφωνα με το άρθρο [18], τα βασικά κριτήρια αξιολόγησης περιλαμβάνουν:

1) Κριτήρια αποδοχής.

Το πλαίσιο ταξινόμησης πρέπει να χρησιμοποιεί λογικούς συλλογισμούς που μπορούν να αποδειχθούν με βάση τις δηλώσεις του ίδιου του πλαισίου και πολύ περισσότερο να μην περιέχει αντιφάσεις.

2) Κριτήριο απτότητας

Οι παράμετροι και οι ιδιότητες της ταξινομημένης επίθεσης που χρησιμοποιούνται για τον ορισμό της κατηγοριοποίησης των κανόνων πρέπει να έχουν όλες τις ακόλουθες ιδιότητες: α) να χρησιμοποιούν ορολογία, η οποία είναι καλά καθορισμένη και καθολικά αποδεκτή από την επιστημονική κοινότητα· β) να μπορούν είτε να μετρηθούν είτε να υπολογίζονται από ένα σύνολο μετρούμενων μεταβλητών ή να καθορίζεται ως συμβάν έτσι ώστε να έχει έγκυρη σχέση αιτίας και αποτελέσματος η επίθεση.

3) Κριτήριο πληρότητας.

Η ταξινόμηση θα πρέπει να παρέχει τα καλύτερα μέχρι σήμερα και πιο πρόσφατα εργαλεία για την ταξινόμηση οποιασδήποτε επίθεσης. Αυτό το κριτήριο γενικεύει την ιδέα της πληρότητας, και διαχωρίζει την απαίτηση για σαφείς διαδικασίες από την προσθήκη κανόνων κατηγοριοποίησης για νέες επιθέσεις ως ξεχωριστό κριτήριο για την επεκτασιμότητα, που ορίζεται παρακάτω. Η ταξινόμηση πρέπει να παρέχει ένα ενημερωμένο εργαλείο για την ταξινόμηση κάθε επίθεσης.

4) Κριτήριο για την επεκτασιμότητα

Ούτε η ίδια η ταξινόμηση ούτε κανένας από τους προκαθορισμένους κανόνες δεν πρέπει ν εμποδίζει την προσθήκη νέων και καινοτόμων κανόνων κατηγοριοποίησης, εκτός εάν αυτοί από μόνοι τους αποτρέψουν προσθήκη νέων κανόνων ή εκτός εάν παραβιάζουν το κριτήριο της αποδοχής. Με άλλα λόγια η προσθήκη νέων κανόνων ταξινόμησης δεν εμποδίζεται εφόσον δεν παραβιάζονται οι κοινώς αποδεκτοί προηγούμενοι.

5) Κριτήριο επάρκειας ορισμών.

Οι κανόνες και οι ορισμοί που αφορούν στην ταξινόμηση θα πρέπει να ορίζονται ιεραρχικά. Δεν πρέπει να είναι δυνατή η παρερμηνεία κανόνων που ορίζουν την ταξινόμηση, όταν αυτοί οι κανόνες διαβάζονται σε συνδυασμό με όλους τους άλλους κανόνες, που προηγούνται του εν λόγω κανόνα. Σε συνδυασμό με το κριτήριο της απτότητας, αυτό το κριτήριο καλύπτει επίσης τον ορισμό του κριτηρίου της κατανοητότητας.

6) Κριτήριο Αποκλειστικότητας.

Ο όρος «κριτήριο αποκλειστικότητας απειλών κυβερνοασφαλείας» αναφέρεται στα κριτήρια που χρησιμοποιούνται για να προσδιορίσουν ποιες απειλές στον κυβερνοχώρο

είναι σημαντικές και ποια από αυτές θα πρέπει να αντιμετωπιστούν ως πρώτης προτεραιότητας. Αυτά τα κριτήρια συνήθως βασίζονται σε διάφορους παράγοντες, όπως:

- Σοβαρότητα και αντίκτυπος: Η έκταση της ζημιάς που μπορεί να προκαλέσει η απειλή σε υποδομές, δεδομένα ή λειτουργίες. Αν η απειλή μπορεί να προκαλέσει σοβαρές συνέπειες, θα είναι πιο πιθανό να την θεωρήσουμε ως κρίσιμη.
- Πιθανότητα εμφάνισης: Πόσο πιθανό είναι να εκδηλωθεί η απειλή, βάσει των διαθέσιμων δεδομένων και της τάσης που δείχνει η απειλή στον κυβερνοχώρο.
- Στόχοι και κίνητρα: Αν η απειλή είναι στοχευμένη ή αν φαίνεται να είναι γενική. Οι απειλές που επικεντρώνονται σε συγκεκριμένους τομείς ή οργανισμούς με υψηλές αξίες (π.χ. τράπεζες ή κυβερνητικές υπηρεσίες) έχουν υψηλότερη προτεραιότητα.
- Διαρκής επικαιροποίηση των απειλών: Ο κόσμος της κυβερνοασφάλειας εξελίσσεται συνεχώς με νέες τεχνικές και απειλές. Οι οργανισμοί παρακολουθούν συνεχώς νέες εξελίξεις για να κατανοήσουν ποιες απειλές είναι πιο πιθανό να συμβούν.
- Διαθεσιμότητα πόρων: Η δυνατότητα των οργανισμών να αντεπεξέλθουν στην απειλή με τους διαθέσιμους πόρους τους (τεχνολογία, ανθρώπινο δυναμικό κλπ.).

7) Κριτήριο Ευελιξίας.

Οι κανόνες που ορίζουν την ταξινόμηση δεν θα πρέπει να επιβάλλουν τη χρήση συγκεκριμένων παραμέτρων ή ιδιοτήτων της επίθεσης, καθώς αυτές οι ιδιότητες ενδέχεται να κάνουν τελικά αδύνατη την ταξινόμηση λόγω αδυναμίας μέτρησης τέτοιων παραμέτρων σε συγκεκριμένες περιπτώσεις χρήσης. Αντίθετα όταν είναι δυνατόν οι κανόνες της ταξινόμησης θα πρέπει να παρέχουν περισσότερα εργαλεία για τη μείωση του συνόλου παραμέτρων, που θα διευκολύνουν την προσαρμογή της ήδη υπάρχουσας επιστημονικής γνώσης στη νέα περίπτωση χρήσης τους. Μπορούμε να πούμε ότι εάν η ταξινόμηση ικανοποιεί το κριτήριο της ευελιξίας τότε μπορεί να προσαρμοστεί για να παρέχει τη μέγιστη χρησιμότητα σε περίπτωση χρήσης του.

2.5 Αρχιτεκτονική Συστημάτων Ασφαλείας

Ο σχεδιασμός μιας αρχιτεκτονικής ασφάλειας αποτελεί θεμελιώδες στοιχείο για την προστασία κάθε τεχνολογικού συστήματος από απειλές και επιθέσεις. Πριν εξεταστεί η εφαρμογή της ασφάλειας σε συστήματα SCADA, κρίνεται απαραίτητο να παρουσιαστούν οι γενικές αρχές που διέπουν την κατασκευή μιας ασφαλούς αρχιτεκτονικής, ανεξαρτήτως εφαρμοστικού περιβάλλοντος.

Η αρχιτεκτονική αυτή ακολουθεί μια πολυεπίπεδη προσέγγιση, στην οποία κάθε επίπεδο ενσωματώνει διαφορετικούς μηχανισμούς ελέγχου και άμυνας, με σκοπό τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. Η προστασία δεν περιορίζεται μόνο στις τεχνικές λύσεις (όπως firewalls ή κρυπτογράφηση), αλλά περιλαμβάνει και πολιτικές ασφάλειας, εκπαίδευση χρηστών, διαχείριση συμβάντων και φυσική προστασία υποδομών.

Η γενική αρχιτεκτονική ενός συστήματος ασφαλείας περιλαμβάνει τα εξής επίπεδα και στοιχεία [11]:

- ***Έλεγχος Πρόσβασης (Authentication & Authorization):*** Χρησιμοποιούνται μηχανισμοί για την ταυτοποίηση των χρηστών και την εξουσιοδότηση των ενεργειών τους μέσα στο σύστημα. Περιλαμβάνει:
  - ✓ Κωδικούς πρόσβασης (passwords)
  - ✓ Μοναδικά αναγνωριστικά χρήστη (user IDs)
  - ✓ Πολιτικές για την ασφαλή χρήση (password policies)
  - ✓ Πολιτικές ελέγχου πρόσβασης (Access Control Lists - ACLs)
  - ✓ Πολιτικές βασισμένες σε ρόλους (Role-Based Access Control - RBAC)
- ***Προστασία Δικτύου (Network Security)***
  - ✓ Τείχη Προστασίας (Firewalls): Διαχωρίζουν το δίκτυο σε ασφαλή και μη ασφαλή τμήματα, ελέγχοντας την εισερχόμενη και εξερχόμενη κίνηση βάσει κανόνων.
  - ✓ Συστήματα Ανίχνευσης και Απόκρισης Εισβολών (IDS/IPS): Ανιχνεύουν και αποτρέπουν πιθανές εισβολές ή κακόβουλες δραστηριότητες στο δίκτυο.
  - ✓ VPN (Virtual Private Networks): Δημιουργούν ασφαλείς συνδέσεις για την προστασία των δεδομένων κατά τη μετάδοση μέσω δημόσιων δικτύων.
  - ✓ Encryption: Η κρυπτογράφηση της κυκλοφορίας δικτύου προστατεύει τα δεδομένα από υποκλοπή ή αλλοίωση.

- ***Ασφάλεια Εφαρμογών (Application Security)***
  - ✓ Ασφαλής Ανάπτυξη Λογισμικού (Secure Software Development): Διασφαλίζει ότι το λογισμικό που αναπτύσσεται είναι απαλλαγμένο από ευπάθειες (π.χ. SQL injection, buffer overflows).
  - ✓ Αξιολόγηση Ευπαθειών και Penetration Testing: Συστηματικοί έλεγχοι για την ανακάλυψη και διόρθωση αδυναμιών πριν την εκμετάλλευσή τους από κακόβουλους χρήστες.
  - ✓ Web Application Firewalls (WAF): Ειδικά τείχη προστασίας για εφαρμογές web που ανιχνεύουν και αποτρέπουν επιθέσεις όπως το SQL Injection ή το Cross-Site Scripting (XSS).
- ***Ασφάλεια Δεδομένων (Data Security)***
  - ✓ Κρυπτογράφηση Δεδομένων (Data Encryption): Εξασφαλίζει ότι τα δεδομένα παραμένουν εμπιστευτικά, τόσο σε κατάσταση αποθήκευσης όσο και κατά τη μετάδοση.
  - ✓ Ασφαλείς Αντίγραφα Ασφαλείας (Backup and Recovery): Διασφαλίζει την ακεραιότητα των δεδομένων και την αποκατάσταση από καταστροφές ή επιθέσεις, όπως ransomware.
  - ✓ Διαχείριση Κλειδιών (Key Management): Διαχειρίζεται τα κρυπτογραφικά κλειδιά με ασφαλή τρόπο.
- ***Ασφάλεια Υποδομών (Infrastructure Security)***
  - ✓ Φυσική Ασφάλεια: Προστασία των φυσικών υποδομών, όπως τα κέντρα δεδομένων, από φυσικές απειλές (π.χ. φωτιά, πλημμύρες).
  - ✓ Ασφάλεια Συσκευών (Endpoint Security): Περιλαμβάνει την προστασία των τελικών συσκευών (υπολογιστές, κινητά, διακομιστές) από επιθέσεις, μέσω antivirus, firewalls, και endpoint detection and response (EDR).
  - ✓ Συνεχής Παρακολούθηση (Continuous Monitoring): Διαρκής παρακολούθηση του συστήματος για τον εντοπισμό ανωμαλιών και την αντίδραση σε συμβάντα ασφαλείας.
- ***Διαχείριση και Επίβλεψη Συμβάντων (Security Incident and Event Management - SIEM)***
  - ✓ SIEM: Ο συνδυασμός εργαλείων και διαδικασιών που βοηθά στη συγκέντρωση, ανάλυση και παρακολούθηση των δεδομένων ασφαλείας από διάφορες πηγές (όπως logs από συστήματα και δίκτυα).

- ✓ Αναφορά και Ανάλυση Συμβάντων: Συλλογή, κατηγοριοποίηση και αντίδραση σε συμβάντα ασφαλείας, με στόχο την αποφυγή ή την ελαχιστοποίηση των επιπτώσεων από τις επιθέσεις.

- ***Ασφάλεια Χρηστών και Ανθρώπινου Παράγοντα (User and Human Factor Security)***
  - ✓ Εκπαίδευση Χρηστών (User Awareness Training): Κατάρτιση των χρηστών για τη σωστή χρήση των συστημάτων και την αναγνώριση επικίνδυνων συμπεριφορών (π.χ. phishing).
  - ✓ Κοινωνική Μηχανική (Social Engineering): Πολιτικές και εκπαιδευτικά προγράμματα που στοχεύουν στην αποφυγή παραπλανητικών επιθέσεων μέσω ανθρώπινων αδυναμιών.
- ***Διαχείριση Κινδύνων και Πολιτικές Ασφαλείας***
  - ✓ Αξιολόγηση Κινδύνων (Risk Assessment): Καθορισμός και αξιολόγηση των πιθανών απειλών, εκτίμηση των κινδύνων και ανάπτυξη στρατηγικών για την αποφυγή ή τον περιορισμό τους.
  - ✓ Πολιτικές Ασφαλείας (Security Policies): Καθορισμός σαφών πολιτικών για τη διαχείριση της ασφάλειας, τις διαδικασίες και τα πρότυπα.
- ***Ευπαθειότητες και Διαχείριση Ενημερώσεων (Vulnerability and Patch Management)***
  - ✓ Ενημερώσεις Λογισμικού (Software Updates): Τακτική αναβάθμιση του λογισμικού για την αντιμετώπιση νέων ευπαθειών που ενδέχεται να εκμεταλλευτούν επιτιθέμενοι.
  - ✓ Διαχείριση Ευπαθειών (Vulnerability Management): Εντοπισμός, εκτίμηση και διόρθωση των αδυναμιών του συστήματος για να μειωθεί ο κίνδυνος επιθέσεων.

2.6 Εργαλεία διερεύνησης Κυβερνοεπιθέσεων

2.6.1 Γενικές παρατηρήσεις

Η διερεύνηση κυβερνοεπιθέσεων αποτελεί κρίσιμο τομέα της κυβερνοασφάλειας, καθώς επιτρέπει την ανίχνευση, την κατανόηση και την αποτροπή κακόβουλων ενεργειών σε πληροφοριακά συστήματα. Στο πλαίσιο αυτό, απαιτείται η χρήση

εξειδικευμένων εργαλείων που υποστηρίζουν τους αναλυτές και τους μηχανισμούς ασφαλείας στον εντοπισμό των ιχνών μιας επίθεσης, στην εκτίμηση της έκτασης της ζημιάς και στην εξαγωγή χρήσιμων συμπερασμάτων για την αποτροπή μελλοντικών περιστατικών. Τα εργαλεία αυτά περιλαμβάνουν τεχνολογίες για την καταγραφή και ανάλυση δεδομένων καταγραφής (logs), την αναγνώριση μη εξουσιοδοτημένων δραστηριοτήτων σε δίκτυα, την παρακολούθηση συστημάτων και τη συσχέτιση μοτίβων επιθέσεων. Σύγχρονες λύσεις ενσωματώνουν και τεχνολογίες τεχνητής νοημοσύνης ή μηχανικής μάθησης, ενισχύοντας τη δυνατότητα πρόβλεψης και ανίχνευσης άγνωστων απειλών.

Η ανάγκη για τέτοια εργαλεία έχει καταστεί ακόμη πιο επιτακτική την τελευταία δεκαετία, λόγω της ραγδαίας εξάπλωσης των δικτύων και της ψηφιοποίησης υπηρεσιών. Ιδιαίτερα κατά την περίοδο της πανδημίας COVID-19, σημειώθηκε αύξηση της κυβερνοεγκληματικότητας κατά 600% [13], πλήττοντας κρίσιμους τομείς, από την εκπαίδευση έως το cloud computing.

Τα εργαλεία διερεύνησης δεν περιορίζονται στον εντοπισμό συμβάντων, αλλά παρέχουν τη δυνατότητα ομαδοποίησης ευπαθειών, ανάλυσης συμπεριφοράς και ανάπτυξης κανόνων συσχέτισης για μελλοντική πρόβλεψη. Για παράδειγμα, μια νέα ευπάθεια μπορεί να προβλεφθεί με ακρίβεια 90% αν εμφανιστούν δύο σχετιζόμενα μοτίβα [19]. Επομένως, η χρήση εξελιγμένων εργαλείων ανάλυσης είναι καθοριστική για την προστασία κρίσιμων πληροφοριακών συστημάτων, όπως τα SCADA, τα οποία απαιτούν real-time αντίδραση, αξιοπιστία και διαλειτουργικότητα με βιομηχανικά πρωτόκολλα και συσκευές [20].

2.6.2 Συστήματα SIEM: Συλλογή και Ανάλυση Δεδομένων Ασφαλείας

Τα συστήματα Security Information and Event Management (SIEM) είναι μια λύση λογισμικού που παρέχει ανάλυση σε πραγματικό χρόνο των δεδομένων του δικτύου. Τα σύστηματα SIEM συλλέγουν δεδομένα από διάφορες πηγές, συμπεριλαμβανομένων συσκευών δικτύου, servers, τελικών σημείων και εφαρμογών. Αυτά τα δεδομένα στη συνέχεια κανονικοποιούνται και αναλύονται για τον εντοπισμό μοτίβων και τάσεων που μπορεί να υποδηλώνουν απειλές για την ασφάλεια. Το σύστημα χρησιμοποιεί προηγμένους αλγόριθμους μηχανικής μάθησης για τον

εντοπισμό ύποπτων συμπεριφορών, όπως μη εξουσιοδοτημένες απόπειρες πρόσβασης, εξαγωγή δεδομένων και μολύνσεις από κακόβουλο λογισμικό [20]. Μόλις εντοπιστεί μια πιθανή απειλή, το σύστημα SIEM δημιουργεί μια ειδοποίηση, η οποία μπορεί να χρησιμοποιηθεί για να ενεργοποιήσει μια αυτοματοποιημένη ενέργεια ή να ειδοποιήσει τους χρήστες για περαιτέρω έρευνα. Αυτό βοηθά τους οργανισμούς να εντοπίζουν προληπτικά και να ανταποκρίνονται σε συμβάντα ασφαλείας, καθώς και να συμμορφώνονται με τους κανονισμούς ασφαλείας.

Εκτός από την παρακολούθηση και την ανίχνευση απειλών σε πραγματικό χρόνο, τα συστήματα SIEM παρέχουν επίσης δυνατότητες όπως διαχείριση αρχείων καταγραφής, αναφορά συμμόρφωσης και εγκληματολογική ανάλυση. Παρέχοντας μια κεντρική προβολή των συμβάντων ασφαλείας σε ολόκληρη την υποδομή ενός οργανισμού, τα συστήματα SIEM επιτρέπουν στους οργανισμούς να εντοπίζουν και να ανταποκρίνονται γρήγορα σε συμβάντα ασφαλείας, μειώνοντας τον κίνδυνο παραβιάσεων δεδομένων και άλλων επιθέσεων στον κυβερνοχώρο.

Τα δύο κύρια στοιχεία του SIEM είναι:

1. **SIEM agent**: είναι ένα λογισμικό που εγκαθίσταται σε ένα σύστημα υπολογιστή ή μια συσκευή προκειμένου να συλλέγει και να αναλύει δεδομένα που σχετίζονται με την ασφάλεια. Λειτουργεί παρακολουθώντας τα αρχεία καταγραφής του συστήματος, την κυκλοφορία δικτύου και άλλες πηγές δεδομένων που σχετίζονται με την ασφάλεια, προκειμένου να ανιχνεύσει πιθανά περιστατικά ή ανωμαλίες ασφάλειας. Ο agent συλλέγει δεδομένα και τα στέλνει στον SIEM server. .Επίσης πολύ σημαντικό είναι ότι έχει τη δυνατότητα να μας δώσει αναλυτικά στοιχεία σε παραγματικό χρόνο για τα συμβάντα έτσι ώστα να υπάρχει βοήθεια για τον εντοπισμό των απειλών χωρίς να προκληθεί κάποια βλάβη. Τα δεδομένα που συλλέγονται είναι χρήσιμα για τις έρευνες των κυβερνοεπιθέσεων, καθώς βοηθούν τους χρήστες να κατανοήσουν καλύτερα το εύρος και τον αντίκτυπο του συμβάντος.
2. **SIEM server**: είναι μια κεντρική πλατφόρμα που συλλέγει, αναλύει και αποθηκεύει δεδομένα ασφαλείας από διάφορες πηγές, κυρίως από τον SIEM agent. Η κύρια λειτουργία ενός server SIEM είναι να προσφέρει μια ενιαία εικόνα της ασφάλειας του οργανισμού και να βοηθήσει τις ομάδες ασφαλείας να διαχειριστούν και να απαντήσουν σε απειλές ή επιθέσεις. Οι servers SIEM χρησιμοποιούν συνήθως έναν συνδυασμό διαχείρισης αρχείων καταγραφής,

συσχέτισης συμβάντων ασφαλείας και προηγμένων αναλυτικών στοιχείων για τον εντοπισμό και την απόκριση σε συμβάντα ασφαλείας σε πραγματικό χρόνο. Μόλις συλλεχθούν τα δεδομένα, ο server SIEM τα επεξεργάζεται και τα αναλύει για να εντοπίσει συμβάντα και μοτίβα ασφαλείας που μπορεί να υποδηλώνουν πιθανή απειλή για την ασφάλεια. Στη συνέχεια, αυτά τα συμβάντα ιεραρχούνται με βάση τη σοβαρότητα και τη σημασία τους και δημιουργούνται ειδοποιήσεις για να ενημερωθεί το προσωπικό ασφαλείας για πιθανές παραβιάσεις της ασφάλειας. Εκτός από τον εντοπισμό και την απόκριση σε απειλές, οι servers SIEM παρέχουν επίσης κεντρική αποθήκευση για αρχεία καταγραφής και συμβάντα ασφαλείας, τα οποία μπορούν να χρησιμοποιηθούν για τις αναφορές και για την ανάλυση εγκληματολογικής έρευνας.

Τα κύρια SIEM εργαλεία είναι:

1. **Wazuh**: open-source SIEM σύστημα που συνδυάζει ανίχνευση εισβολών (IDS), έλεγχο ακεραιότητας αρχείων, ανάλυση logs και συμμόρφωση με πολιτικές ασφαλείας. Υποστηρίζει εγκατάσταση ελαφριών agents σε συσκευές περιορισμένων πόρων (όπως RTUs και edge servers), γεγονός που το καθιστά ιδανικό για περιβάλλοντα SCADA. Ενσωματώνεται άψογα με τον Elastic Stack για προηγμένες δυνατότητες απεικόνισης και συσχέτισης συμβάντων. [29]
2. **OSSIM**: open-source λύση της AlienVault που περιλαμβάνει λειτουργίες SIEM, IDS, vulnerability assessment και asset discovery. Παρότι προσφέρει πλούσια λειτουργικότητα, η πλατφόρμα είναι βαριά και η ανάπτυξή της περίπλοκη, ενώ δεν υποστηρίζεται ενεργά σε νέα περιβάλλοντα. Δεν είναι σχεδιασμένο για συσκευές περιορισμένων πόρων, γεγονός που το καθιστά λιγότερο κατάλληλο για SCADA.[34]
3. **Splunk**: εμπορικό εργαλείο SIEM υψηλής απόδοσης, με δυνατότητες machine learning και ανάλυσης μεγάλων όγκων δεδομένων. Διαθέτει εξαιρετικό UI και δυνατότητες real-time συσχέτισης γεγονότων. Ωστόσο, το υψηλό του κόστος και η ανάγκη για ισχυρή υποδομή το καθιστούν μη ιδανική επιλογή για SCADA περιβάλλοντα με χαμηλούς πόρους. [35]
4. **Qradar**: κορυφαίο SIEM με δυνατότητες τεχνητής νοημοσύνης μέσω του Watson. Παρέχει ισχυρές δυνατότητες συσχέτισης γεγονότων και threat intelligence, αλλά απαιτεί πολύπλοκη εγκατάσταση και σημαντικούς πόρους.

Παρότι υποστηρίζει OT/ICS περιβάλλοντα, η υποδομή του δεν ταιριάζει με τις απαιτήσεις ευελιξίας και lightweight λειτουργίας ενός τυπικού SCADA συστήματος. [36]

Εργαλείο	**Τύπος - Κόστος**	**AI/ML Υποστήριξη**	**Πλεονεκτήματα**	**Αδυναμίες**	**Καταλληλότητα για SCADA**
Wazuh	Open-source (Δωρεάν)	Ναι (μέσω ELK)	1. Lightweight 2. Ευέλικτο 3. Συμβατό με ELK	Όχι αυτόνομο ML engine	Ιδανική: agents για low-resource συσκευές
OSSIM	Open-source (Δωρεαν)	Περιορισμένα	1. Ολοκληρωμένη λύση 2. IDS + VA	1. Δύσκολη συντήρηση 2. Ξεπερασμένο	Μέτρια: παλιό και βαρύ
Splunk	Εμπορικό (Πολύ ακριβό)	ML toolkit	1. Ισχυρό UI 2. Scalability	1. Ακριβό 2. Υπερβολικό για SCADA	Όχι: απαιτεί ισχυρή υποδομή
QRadar	Εμπορικό (Πολύ ακριβό)	Watson AI	1. Συσχέτιση Απειλών 2. Απεικονιστική Πληροφόρηση Απειλών	1. Πολύπλοκο 2. Απαιτεί resources	Όχι: βαρύ και δύσχρηστο για SCADA πεδίου

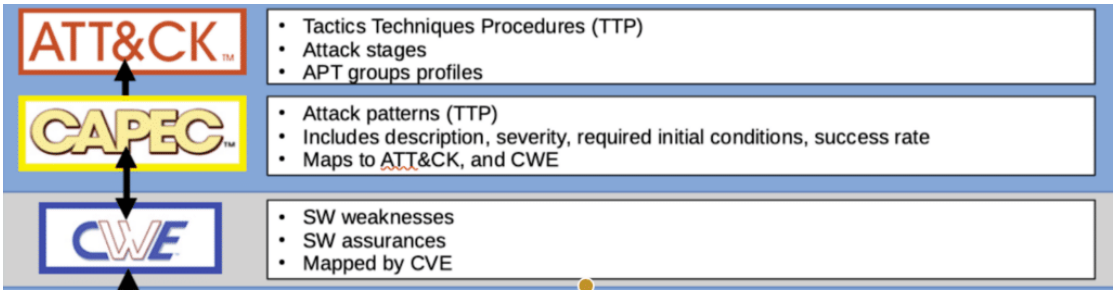
Πίνακας 2.6-i: Συγκριτικός Πίνακας για την επιλογή SIEM

2.6.3 Βάσεις Γνώσης για την Ψηφιακή Εγκληματολογική Διερεύνηση Κυβερνοαπειλών

Η αναγνώριση και η ανάλυση κυβερνοαπειλών δεν βασίζεται αποκλειστικά σε τεχνικά εργαλεία, αλλά και στη συστηματική γνώση των τρόπων επίθεσης. Οι βάσεις γνώσης που περιλαμβάνουν μοτίβα επιθέσεων και κοινές αδυναμίες αποτελούν βασικό εργαλείο στα χέρια των αναλυτών, καθώς τους βοηθούν να εντοπίζουν κινδύνους και να προσαρμόζουν τα συστήματα άμυνας αναλόγως. Σε έναν κόσμο όπου οι επιθέσεις αυξάνονται συνεχώς και εξελίσσονται διαρκώς, η χρήση βιβλιοθηκών που παρέχουν ενημερωμένο και τυποποιημένο περιεχόμενο για απειλές, τεχνικές και ευπάθειες είναι

απαραίτητη. Οι τρεις κυριότερες βάσεις δεδομένων που χρησιμοποιούνται στην κυβερνοασφάλεια είναι:

1. CAPEC (Common Attack Pattern Enumeration and Classification): παρέχει έναν δημόσιο κατάλογο από μοτίβα επιθέσεων που βοηθά τους χρήστες να κατανοήσουν πώς οι αντίπαλοι εκμεταλλεύονται τις αδυναμίες. [30]
2. CWE (Common Weakness Enumeration): είναι μια λίστα κοινών αδυναμιών λογισμικού και υλικού. Γνωρίζοντας τις αδυναμίες που οδηγούν σε τρωτά σημεία σημαίνει ότι οι προγραμματιστές λογισμικού μπορούν να τις εξαλείψουν πριν από την ανάπτυξη, όταν είναι πολύ πιο εύκολο και φθηνότερο να το κάνουν. [31]
3. MITRE ATT&CK: είναι μια ολοκληρωμένη βάση γνώσεων που καταγράφει τις τεχνικές των αντιπάλων, βασισμένη σε πραγματικές παρατηρήσεις από περιστατικά κυβερνοασφάλειας. Εστιάζει στον τρόπο με τον οποίο οι αντίπαλοι αλληλοεπιδρούν με τα συστήματα κατά τη διάρκεια μιας επίθεσης. [32]



Εικόνα 2.6-i: Συσχέτιση πλαισίων MITRE ATT&CK, CAPEC και CWE για την ανάλυση κυβερνοεπιθέσεων. Πηγή: nopsec.com[7]

2.6.4 Αποθήκευση και Ανάλυση Μεγάλων Δεδομένων με HDFS

Σε περιβάλλοντα SCADA, όπου οι συσκευές συλλέγουν συνεχώς δεδομένα από αισθητήρες, RTUs και άλλες μονάδες πεδίου, δημιουργείται τεράστιος όγκος δεδομένων καταγραφής και τηλεμετρίας. Η ανάγκη για αξιόπιστη, κατανεμημένη και ανεκτική σε σφάλματα αποθήκευση είναι κρίσιμη τόσο για τη διαχείριση των καθημερινών λειτουργιών όσο και για την ανάλυση συμβάντων ασφαλείας. Συστήματα όπως τα SIEM, που συγκεντρώνουν logs και δεδομένα από πολλές πηγές, απαιτούν υποδομές ικανές να χειρίζονται μεγάλα δεδομένα με ταχύτητα και ασφάλεια. Σε αυτό

[7] https://www.nopsec.com/blog/mapping-cves-and-attck-framework-ttps-an-empirical-approach/

το πλαίσιο, αξιοποιείται το Hadoop Distributed File System (HDFS) ως βασικό εργαλείο αποθήκευσης και ανάλυσης σε κατανεμημένα περιβάλλοντα.

Σύμφωνα με την επίσημη ιστοσελίδα [33], το Hadoop Distributed File System (HDFS) είναι ένα κατανεμημένο σύστημα αρχείων που έχει σχεδιαστεί για να αποθηκεύει μεγάλα σύνολα δεδομένων σε πολλούς servers. Αποτελεί βασικό στοιχείο του οικοσυστήματος Apache Hadoop, το οποίο παρέχει μια πλατφόρμα για κατανεμημένη επεξεργασία και ανάλυση δεδομένων. Το HDFS είναι εξαιρετικά ανεκτικό σε σφάλματα και έχει σχεδιαστεί για να λειτουργεί σε υλικό χαμηλού κόστους, καθιστώντας το μια δημοφιλή επιλογή για την επεξεργασία μεγάλων δεδομένων. Στο HDFS, τα αρχεία αναλύονται σε μπλοκ και διανέμονται σε πολλούς κόμβους στο σύμπλεγμα. Κάθε μπλοκ αναπαράγεται πολλές φορές για να διασφαλιστεί ο πλεονασμός και η διαθεσιμότητα των δεδομένων.

Οι δυνατότητες ανοχής σφαλμάτων και πλεονασμού δεδομένων διασφαλίζουν ότι τα δεδομένα είναι πάντα διαθέσιμα, ακόμη και σε περίπτωση hardware failure. Το HDFS υποστηρίζει επίσης data locality, πράγμα που σημαίνει ότι οι εργασίες επεξεργασίας μπορούν να εκτελεστούν στους ίδιους κόμβους όπου αποθηκεύονται τα δεδομένα, μειώνοντας την επιβάρυνση του δικτύου και βελτιώνοντας την απόδοση. Τέλος, το HDFS είναι εξαιρετικά επεκτάσιμο, επιτρέποντας στους οργανισμούς να αποθηκεύουν και να επεξεργάζονται petabyte δεδομένων ή περισσότερα. Τα τρία βασικά στοιχεία του HDFS είναι:

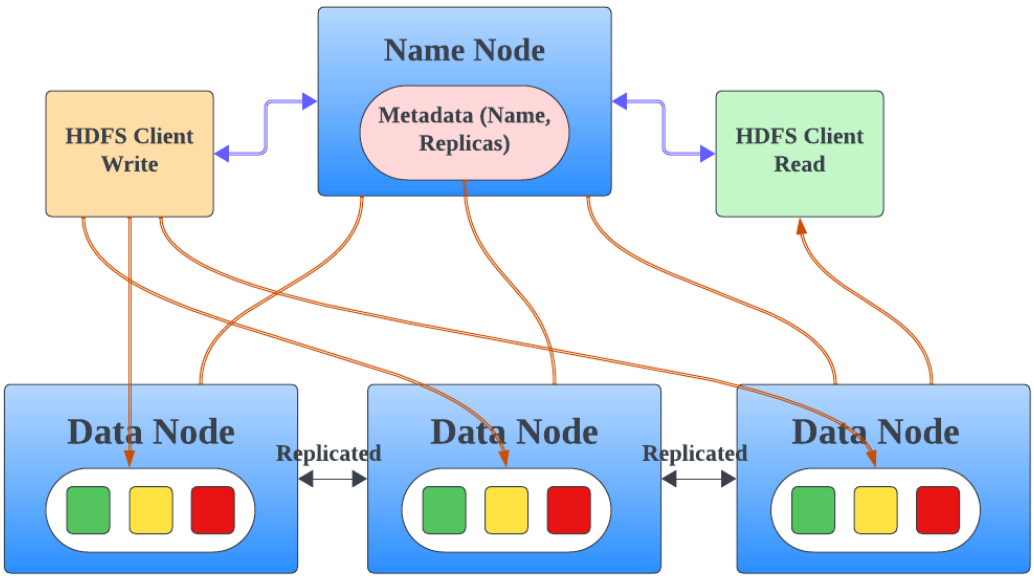
- **NameNode**: είναι υπεύθυνος για τη διατήρηση του namespace tree, την αντιστοίχιση μπλοκ αρχείων σε DataNodes και τη διατήρηση ολόκληρου του χώρου ονομάτων στη μνήμη RAM. Το περιεχόμενο του αρχείου χωρίζεται σε μεγάλα μπλοκ (συνήθως 128 megabyte) και κάθε μπλοκ του αρχείου αναπαράγεται ανεξάρτητα σε πολλούς DataNodes (συνήθως τρεις). Οι HDFS client επικοινωνούν πρώτα με το NameNode για τις θέσεις των μπλοκ δεδομένων που αποτελούν το αρχείο και στη συνέχεια διαβάζουν τα περιεχόμενα του μπλοκ από το DataNode που βρίσκεται πιο κοντά στον client. Κατά την εγγραφή δεδομένων, ο client ζητά από το NameNode να ορίσει μια σουίτα τριών DataNodes για να φιλοξενήσει τα αντίγραφα μπλοκ.
- **DataNode**: είναι υπεύθυνοι για την αποθήκευση των πραγματικών δεδομένων στο σύστημα αρχείων. Κάθε αντίγραφο μπλοκ σε ένα DataNode αντιπροσωπεύεται από δύο αρχεία στο εγγενές σύστημα αρχείων του τοπικού

κεντρικού υπολογιστή. Το πρώτο αρχείο περιέχει τα ίδια τα δεδομένα και το δεύτερο αρχείο είναι τα μεταδεδομένα του μπλοκ, συμπεριλαμβανομένων των αθροισμάτων ελέγχου για τα δεδομένα του μπλοκ και τη σφραγίδα δημιουργίας του μπλοκ. Κατά την εκκίνηση, κάθε DataNode συνδέεται με το NameNode και εκτελεί μια χειραψία. Μετά τη χειραψία, το DataNode καταχωρείται στο NameNode και στέλνει μια αναφορά μπλοκ για να αναγνωρίσει τα αντίγραφα μπλοκ που διαθέτει. Οι heartbeats από τα DataNodes μεταφέρουν πληροφορίες σχετικά με τη συνολική χωρητικότητα αποθήκευσης, το κλάσμα της αποθήκευσης που χρησιμοποιείται και τον αριθμό των μεταφορών δεδομένων που βρίσκονται σε εξέλιξη, οι οποίες χρησιμοποιούνται για την κατανομή χώρου του NameNode και τις αποφάσεις εξισορρόπησης φορτίου.

- **HDFS client**: είναι μια βιβλιοθήκη κωδικών που παρέχει μια διεπαφή για τις εφαρμογές χρήστη για την αλληλεπίδραση με το σύστημα αρχείων HDFS. Ο client επικοινωνεί με το NameNode για να ανακτήσει τις θέσεις των μπλοκ δεδομένων που αποτελούν ένα αρχείο και στη συνέχεια διαβάζει τα περιεχόμενα του μπλοκ από τον πλησιέστερο DataNode. Κατά την εγγραφή δεδομένων, ο client ζητά από το NameNode να ορίσει μια σουίτα τριών DataNodes για να φιλοξενήσει τα αντίγραφα του μπλοκ και στη συνέχεια γράφει δεδομένα στους DataNodes με τρόπο διοχέτευσης. Ακόμα, χειρίζεται λειτουργίες συστήματος αρχείων, όπως δημιουργία, διαγραφή και μετονομασία αρχείων και καταλόγων, αλλαγή αδειών αρχείων και ρύθμιση ορίων χώρου στο δίσκο. Τέλος, η βιβλιοθήκη μπορεί να χρησιμοποιηθεί από άλλα στοιχεία Hadoop όπως το MapReduce και το HBase για ανάγνωση και εγγραφή δεδομένων από το HDFS.

Σύμφωνα με την τελευταία έκδοση της Apache Hadoop 3.3.5, υπάρχει μια νέα ρύθμιση που λέγεται HDFS High Availability. Στην παλιά έκδοση Hadoop 2.0.0, ο server NameNode ήταν single point of failure (SPOF). Σε κάθε κατηγοριοποίηση υπήρχε μόνο ένας server NameNode και σε περίπτωση αποτυχίας το σύστημα δεν λειτουργούσε μέχρι την επαναφορά του. Το πρόβλημα θα δημιουργούταν ακόμα και με μια αναβάθμιση λογισμικού. Πλέον με το HDFS High Availability καταφέρνει και λύνει το πρόβλημα SPOF, έχοντας 2 ή περισσότερους NameNodes. Ο ένας server χαρακτηρίζεται ως Active και οι υπόλοιποι ως Passive ή Standby.

Σε οποιαδήποτε στιγμή ένας server μπαίνει σε κατάσταση Active και οι υπόλοιποι Passive. Ο Active NameNode είναι υπεύθυνος για όλους τους client της κατηγοριοποίησης, ενώ οι Passive παραμένουν στην ίδια κατάσταση μέχρι να αποτύχει ο Active NameNode.



Εικόνα 2.6-ii: Αρχιτεκτονική του HDFS (Hadoop Distributed File System). Πηγή: medium.com[8]

2.6.5 Automated Forensic Tool: Πολυεπίπεδο Εργαλείο Ανάλυσης Συμβάντων Ασφαλείας

Η ανάλυση και τεκμηρίωση συμβάντων ασφαλείας σε περιβάλλοντα SCADA απαιτεί τη χρήση εργαλείων που συνδυάζουν ακρίβεια, ταχύτητα και πρόσβαση σε εξωτερικές βάσεις γνώσης. Οι σύγχρονες υποδομές επιτήρησης, όπως τα SIEM, μπορούν να παρέχουν πολύτιμα δεδομένα, ωστόσο η ερμηνεία και η συσχέτισή τους απαιτεί πιο εξειδικευμένη προσέγγιση. Πρόκειται για ένα πολυεπίπεδο εργαλείο ανάλυσης, το οποίο συνεργάζεται με ένα SIEM σύστημα και αξιοποιεί εξωτερικές βιβλιοθήκες επιθέσεων, όπως το CAPEC, το MITRE ATT&CK και το CVE, προκειμένου να εμπλουτίσει τις αναφορές ασφαλείας με στοχευμένη πληροφορία. Η

[8] https://medium.com/@venkatkarthick15/understanding-hdfs-a-simple-guide-to-how-hadoop-stores-data-51c1a29e1f73

αρχιτεκτονική του βασίζεται σε τέσσερα διακριτά επίπεδα, καθένα από τα οποία επιτελεί εξειδικευμένο ρόλο στην ερμηνεία και κατηγοριοποίηση των κυβερνοεπιθέσεων.

Σύμφωνα με το άρθρο [20], το Automated Forensic Tool είναι μια αρχιτεκτονική πολλαπλών παραγόντων που λαμβάνει αναφορές από κάποιο SIEM εργαλείο και στοχεύει στην υποστήριξη των χρηστών κατά τη διερεύνηση συμβάντων ασφαλείας. Το εργαλείο εμπλουτίζει το συμβάν ασφαλείας με γνωστές βάσεις δεδομένων (CAPEC, MITER ATT&CK και CVE) για να παρέχει ένα λεπτομερές πλαίσιο της επίθεσης. Τα τέσσερα επίπεδα (layers) του Automated Forensic Tool είναι:

1. Data Collector layer: (Επίπεδο Συλλογής Δεδομένων) Είναι το μέρος μιας αρχιτεκτονικής συστήματος ή εφαρμογής που είναι υπεύθυνο για τη συλλογή και την αποθήκευση δεδομένων από διάφορες πηγές, όπως συσκευές, εφαρμογές ή συστήματα. Αυτά τα δεδομένα μπορεί να περιλαμβάνουν πληροφορίες για τη λειτουργία του συστήματος, τα δεδομένα χρηστών, logs, metrics, ή οποιοδήποτε άλλο είδος πληροφορίας που χρειάζεται για ανάλυση ή παρακολούθηση.

2. Artificial Intelligence (AI) layer: είναι υπεύθυνο για τον εμπλουτισμό της αναφοράς από το προηγούμενο layer με τις βάσεις δεδομένων ή άλλα συμβάντα. Το επίπεδο αυτό χρησιμοποιεί μηχανική εκμάθηση και τεχνικές NLP όπως η ομαδοποίηση και το tf-idf για να κάνει συσχετισμούς μεταξύ συμβάντων ασφαλείας και σχετικών βάσεων δεδομένων.
3. Forensic Intelligence Layer: είναι υπεύθυνο για την παροχή ενός λεπτομερούς προφίλ αυτού που κάνει επίθεση το οποίο περιλαμβάνει τις πηγές και τις δεξιότητες που απαιτούνται για την έναρξη της επίθεσης καθώς και μερικές λύσεις του προβλήματος. Αυτό το επίπεδο χρησιμοποιεί τα μοτίβα επίθεσης από το AI layer για να εξάγει πληροφορίες και εμφανίζει τα σχετικά συμβάντα για να βοηθήσει τους χρήστες να εξετάσουν τις σχέσεις μεταξύ των συμβάντων. Ακόμα, επιτρέπει στους χρήστες να κατηγοριοποιούν και να ιεραρχούν τα συμβάντα ασφαλείας ως συμβάντα με βάση τον τύπο της εγκληματολογικής έρευνας που απαιτείται. Τα περιστατικά ταξινομούνται σε διάφορες κατηγορίες με βάση τη σοβαρότητα του συμβάντος.

4. Front-end GUI layer: (Επίπεδο Εμφάνισης Χρήστη ή Επίπεδο Διεπαφής Χρήστη) Έχει να κάνει με το κομμάτι ενός συστήματος ή εφαρμογής που είναι υπεύθυνο για την αλληλεπίδραση με τον χρήστη μέσω μιας γραφικής διεπαφής χρήστη (GUI). Το GUI είναι το περιβάλλον που βλέπει ο χρήστης και με το οποίο αλληλεπιδρά, χρησιμοποιώντας στοιχεία όπως κουμπιά, παράθυρα, μενού, φόρμες, και άλλα γραφικά στοιχεία.

3 *Προτεινόμενη αρχιτεκτονική*

3.1 Σκοπός και βασικές αρχές

Η προηγούμενη ανάλυση ανέδειξε το πολυδιάστατο φάσμα εργαλείων, τεχνικών και υποδομών που χρησιμοποιούνται σήμερα για τη διερεύνηση κυβερνοαπειλών και την ενίσχυση της ασφάλειας σε πληροφοριακά συστήματα. Ωστόσο, όταν πρόκειται για συστήματα SCADA – τα οποία αποτελούν κρίσιμες υποδομές για τη λειτουργία της βιομηχανίας, της ενέργειας, των μεταφορών και άλλων τομέων – η ανάγκη για εξειδικευμένες, συνδυαστικές και σε βάθος προσαρμόσιμες αρχιτεκτονικές καθίσταται επιτακτική. Παρότι εργαλεία όπως τα συστήματα SIEM, οι πλατφόρμες big data και οι βάσεις δεδομένων κυβερνοαπειλών προσφέρουν σημαντικές δυνατότητες, η ενσωμάτωσή τους σε ενιαία λειτουργική αρχιτεκτονική που να ανταποκρίνεται στις ιδιαιτερότητες των SCADA (όπως η real-time παρακολούθηση, η δυσκολία αναβάθμισης και οι απαιτήσεις υψηλής διαθεσιμότητας) παραμένει περιορισμένη.

Η προτεινόμενη αρχιτεκτονική επιχειρεί να καλύψει αυτό το κενό, προτείνοντας ένα ολιστικό και κατανεμημένο σύστημα ανάλυσης και απόκρισης σε κυβερνοαπειλές, ειδικά σχεδιασμένο για SCADA. Συνδυάζει εργαλεία όπως το Wazuh (SIEM), το HDFS (για αποθήκευση και διαχείριση μεγάλων δεδομένων) και το Automated Forensic Tool για εγκληματολογική διερεύνηση και εμπλουτισμό των περιστατικών ασφαλείας με πληροφορία από διεθνείς βάσεις όπως το MITRE ATT&CK και το CAPEC.

Η καινοτομία της πρότασης δεν έγκειται μόνο στη χρήση των επιμέρους τεχνολογιών, αλλά κυρίως στον τρόπο ενοποίησής τους σε ένα ευέλικτο, επεκτάσιμο και αποδοτικό σχήμα, το οποίο μπορεί να προσαρμοστεί σε διαφορετικές περιπτώσεις χρήσης εντός SCADA υποδομών. Στις επόμενες υποενότητες παρουσιάζεται η αρχιτεκτονική, η λειτουργική της δομή και ο τρόπος με τον οποίο υποστηρίζει την ενίσχυση της ασφάλειας και της επιχειρησιακής ανθεκτικότητας.

Η προτεινόμενη αρχιτεκτονική για την ανίχνευση και διερεύνηση κυβερνοεπιθέσεων σε συστήματα SCADA βασίζεται στη συνδυασμένη χρήση παραδοσιακών υποσυστημάτων SCADA και σύγχρονων εργαλείων κυβερνοασφάλειας. Η επιλογή των τεχνολογικών στοιχείων έγινε με κριτήριο την ενίσχυση της ικανότητας εντοπισμού απειλών, την επεξεργασία μεγάλου όγκου δεδομένων και τη δυνατότητα

διερεύνησης περιστατικών με τρόπο που να ανταποκρίνεται στις ιδιαίτερες απαιτήσεις των SCADA περιβαλλόντων. Παρακάτω παρουσιάζονται τα βασικά στοιχεία της αρχιτεκτονικής και η συνεισφορά τους στο συνολικό μοντέλο.

3.2 Δομικά Στοιχεία

3.2.1 Συσκευές Πεδίου και Ελεγχόμενος Εξοπλισμός

Οι συσκευές πεδίου αποτελούν το χαμηλότερο και πιο κρίσιμο επίπεδο της αρχιτεκτονικής SCADA, καθώς είναι υπεύθυνες για την παρακολούθηση και τον έλεγχο εξοπλισμού στο φυσικό πεδίο λειτουργίας. Στην παρούσα αρχιτεκτονική περιλαμβάνονται RTUs (Remote Terminal Units), PLCs (Programmable Logic Controllers) και IEDs (Intelligent Electronic Devices), τα οποία είναι υπεύθυνα για τη συλλογή δεδομένων και την εκτέλεση τοπικών εντολών. Οι συσκευές αυτές ελέγχουν και επικοινωνούν με αισθητήρες (όπως αισθητήρες θερμοκρασίας, πίεσης ή στάθμης), ενεργοποιητές (όπως βαλβίδες ή μοτέρ), καθώς και με άλλες μονάδες πεδίου, όπως μετρητές και διακόπτες ισχύος. Τα δεδομένα που συλλέγονται από τον εξοπλισμό αυτό προωθούνται σε πραγματικό χρόνο στο ανώτερο επίπεδο του συστήματος (MTU), υποστηρίζοντας την εποπτεία, τη λήψη αποφάσεων και την ανάλυση συμβάντων ασφαλείας.

Η ενσωμάτωσή τους στην αρχιτεκτονική είναι απαραίτητη, καθώς αποτελούν την κύρια πηγή πληροφοριών για την κατάσταση και τη λειτουργία του συστήματος, και επιτρέπουν την ανίχνευση αποκλίσεων ή ενδείξεων κακόβουλων ενεργειών σε πρώιμο στάδιο. Επιπλέον, δεδομένου ότι οι συσκευές αυτές βρίσκονται απευθείας εκτεθειμένες στο πεδίο και συχνά λειτουργούν με περιορισμένους μηχανισμούς προστασίας, αποτελούν και ένα από τα πιο ευάλωτα σημεία της συνολικής υποδομής SCADA.

3.2.2 Κεντρικό Σύστημα Ελέγχου

Το Κεντρικό Σύστημα Ελέγχου αποτελεί τον βασικό κόμβο λήψης αποφάσεων και επεξεργασίας δεδομένων στην αρχιτεκτονική SCADA. Περιλαμβάνει τις λειτουργικές μονάδες:

- **MTU:** διαχειρίζεται τη συλλογή δεδομένων από τις συσκευές πεδίου μέσω των RTUs/PLCs και συντονίζει την αποστολή εντολών ελέγχου στο πεδίο. Αποτελεί την κύρια διεπαφή με τις απομακρυσμένες μονάδες, εξασφαλίζοντας την εποπτεία και τον συγχρονισμό των λειτουργιών σε πραγματικό χρόνο.
- **HMI:** επιτρέπει στον ανθρώπινο χειριστή να παρακολουθεί την κατάσταση του συστήματος μέσω γραφικής απεικόνισης, ενώ του δίνει και τη δυνατότητα χειροκίνητης παρέμβασης σε κρίσιμες καταστάσεις. Παράλληλα, παρέχει πρόσβαση σε ειδοποιήσεις, συναγερμούς και στατιστικά δεδομένα λειτουργίας.
- **Historian:** αναλαμβάνει την αποθήκευση ιστορικών δεδομένων λειτουργίας. Τα δεδομένα αυτά μπορούν να αξιοποιηθούν για ανάλυση αποκλίσεων, διερεύνηση περιστατικών ασφαλείας και συσχέτιση με άλλα στοιχεία που καταγράφονται στο σύστημα.

Στο πλαίσιο της προτεινόμενης αρχιτεκτονικής, το κεντρικό αυτό υποσύστημα διαδραματίζει κρίσιμο ρόλο στη γρήγορη ανίχνευση και αντιμετώπιση επιθέσεων, καθώς αποτελεί το σημείο συγκέντρωσης και διαβίβασης όλων των λειτουργικών και καταγραφικών δεδομένων. Για τον λόγο αυτό, η ενίσχυσή του με κατάλληλα εργαλεία παρακολούθησης και ανάλυσης κρίνεται απαραίτητη, ώστε να διασφαλίζεται η αποδοτικότητα και η ασφάλεια της συνολικής αρχιτεκτονικής.

3.2.3 Υποσύστημα Δικτυακής Επικοινωνίας

Το υποσύστημα δικτυακής επικοινωνίας επιτρέπει την ανταλλαγή δεδομένων μεταξύ των συσκευών πεδίου και του κεντρικού συστήματος ελέγχου, καθώς και μεταξύ άλλων κρίσιμων μονάδων της αρχιτεκτονικής. Η σωστή λειτουργία του είναι απαραίτητη για τη μετάδοση δεδομένων λειτουργίας, καταγραφών και εντολών ελέγχου σε πραγματικό χρόνο. Η επικοινωνία βασίζεται σε βιομηχανικά πρωτόκολλα, όπως το Modbus, το DNP3 και το IEC 60870-5-104, τα οποία είναι ευρέως διαδεδομένα σε SCADA περιβάλλοντα. Τα πρωτόκολλα αυτά έχουν σχεδιαστεί για αξιοπιστία και χαμηλή καθυστέρηση, αν και πολλές φορές λειτουργούν χωρίς ενσωματωμένα χαρακτηριστικά ασφάλειας.

Αν και η διπλωματική εργασία δεν εστιάζει σε βάθος στην ασφάλεια των δικτυακών επικοινωνιών, αναγνωρίζεται ότι αποτελεί σημείο κρίσιμης σημασίας, όπου πρέπει να εφαρμόζονται ευρέως αποδεκτές πολιτικές ασφαλείας, όπως ο έλεγχος πρόσβασης, η λογική διαχείριση ροής δεδομένων, και η τμηματοποίηση δικτύου. Αυτές οι πρακτικές

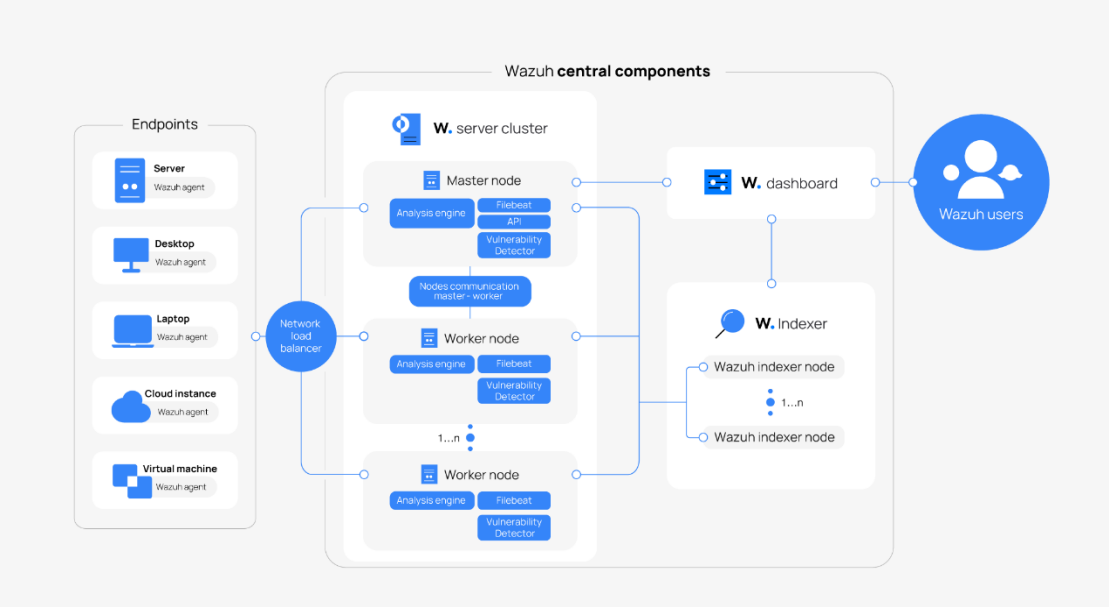
μπορούν να περιορίσουν την έκθεση σε απειλές και να ενισχύσουν τη συνολική ανθεκτικότητα της αρχιτεκτονικής.

3.2.4 Wazuh – Σύστημα Ανίχνευσης και Ανάλυσης Συμβάντων

Στο προτεινόμενο μοντέλο, ο ρόλος της ανίχνευσης και ανάλυσης συμβάντων ασφαλείας ανατίθεται στο Wazuh, ένα ανοιχτού κώδικα SIEM εργαλείο που συνδυάζει λειτουργίες ανίχνευσης εισβολών, ανάλυσης logs και συμμόρφωσης με πολιτικές ασφαλείας. Το Wazuh επιλέχθηκε με βάση τις ειδικές απαιτήσεις που θέτουν τα περιβάλλοντα SCADA, όπου η ανάγκη για real-time παρακολούθηση, χαμηλό αποτύπωμα στα άκρα του συστήματος και επεκτασιμότητα είναι κρίσιμες.

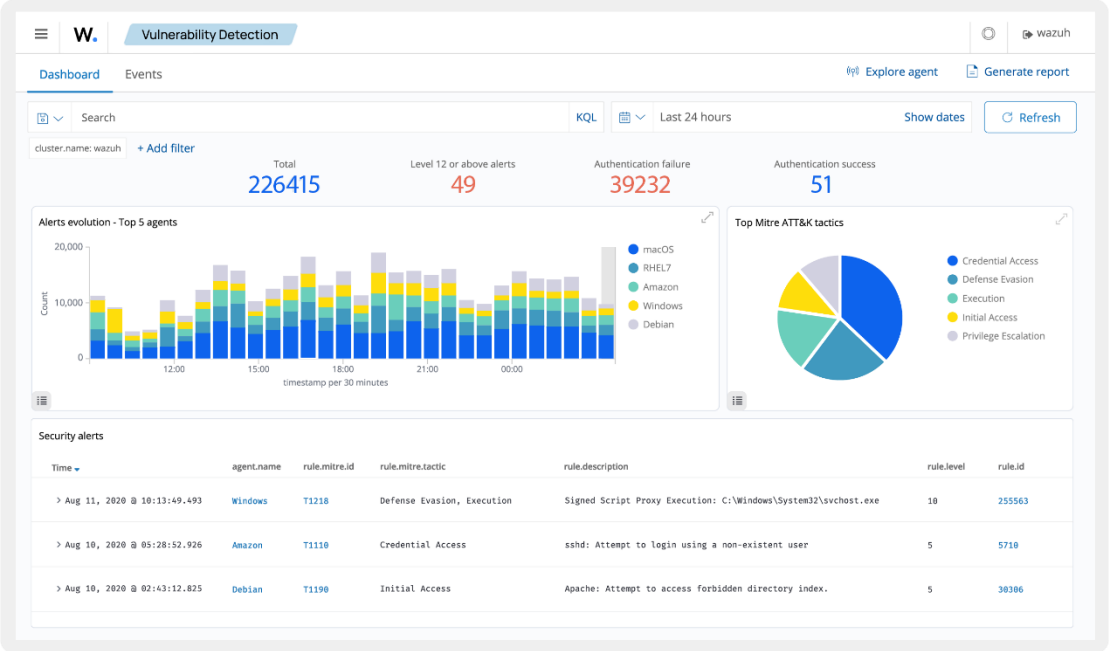
Η ενσωμάτωσή του στην αρχιτεκτονική λειτουργεί σε δύο επίπεδα:

1. **Τοπικά**, μέσω των agents που παρακολουθούν log αρχεία, επιτελούν integrity checking και εντοπίζουν ανωμαλίες συμπεριφοράς.
2. **Κεντρικά**, μέσω του SIEM server που δέχεται, αναλύει και συσχετίζει τα δεδομένα από όλο το σύστημα, παρέχοντας ειδοποιήσεις και αναφορές.



Εικόνα 3.2-i: Αρχιτεκτονική Wazuh. Πηγή: wazuh[9]

[9] https://wazuh.com/



Εικόνα 3.2-ii: Πίνακας Ελέγχου Wazuh. Πηγή: wazuh[10]

3.2.5 HDFS – Σύστημα Αποθήκευσης και Ανάλυσης Δεδομένων –

Για την αποθήκευση και ανάλυση των δεδομένων ασφαλείας που συλλέγονται από τις διάφορες μονάδες του συστήματος SCADA, η αρχιτεκτονική αξιοποιεί το Hadoop Distributed File System (HDFS). Η επιλογή του HDFS βασίζεται στην ανάγκη διαχείρισης μεγάλων όγκων δεδομένων (Big Data), που παράγονται σε πραγματικό χρόνο από τις συσκευές πεδίου, το κεντρικό σύστημα ελέγχου και τα εργαλεία ανάλυσης.

Το HDFS παρέχει ένα κατανεμημένο μοντέλο αποθήκευσης που εξασφαλίζει πλεονασμό, ανοχή σε σφάλματα και επεκτασιμότητα. Σε περιβάλλοντα SCADA, όπου απαιτείται σταθερή απόδοση και υψηλή διαθεσιμότητα, το HDFS προσφέρει αξιοπιστία ακόμη και σε περιπτώσεις υλικών βλαβών ή αυξημένου φορτίου.

Η αποδοτικότητα του HDFS έχει μελετηθεί σε διάφορα περιβάλλοντα, με χαρακτηριστικό παράδειγμα το Yahoo, όπου πραγματοποιήθηκαν benchmarks για την αξιολόγηση των επιδόσεων σε μεγάλα clusters [14]. Το πείραμα που περιγράφεται είναι μια δοκιμή επιδόσεων (benchmark), η οποία μετρά τον μέσο ρυθμό μεταφοράς

[10] https://wazuh.com/

δεδομένων για λειτουργίες ανάγνωσης, εγγραφής και τροποποίησης αρχείων στο HDFS. Αυτό το πείραμα εκτελείται με τη χρήση του DFSIO, μιας εφαρμογής που είναι διαθέσιμη ως μέρος της διανομής του Hadoop. Το πείραμα σχεδιάστηκε για να μετρήσει την απόδοση μόνο κατά τη διάρκεια της μεταφοράς δεδομένων. Τα αποτελέσματα ήταν θετικά για δύο κύριους λόγους:

- Υψηλή θύρα διέλευσης: Τα αποτελέσματα έδειξαν ότι η μέση θύρα διέλευσης για την ανάγνωση και την εγγραφή σε αρχεία στο HDFS ήταν υψηλή. Για παράδειγμα, η μέση θύρα διέλευσης για ανάγνωση ήταν 66 MB / δευτερόλεπτο ανά κόμβο, ενώ για εγγραφή ήταν 40 MB / δευτερόλεπτο ανά κόμβο. Αυτό υποδεικνύει ότι το HDFS μπορεί να διαχειριστεί αποτελεσματικά την ανάγνωση και την εγγραφή μεγάλων όγκων δεδομένων.
- Κλιμάκωση με τον αριθμό των κόμβων: Το πείραμα εκτελέστηκε σε clusters των τουλάχιστον 3500 κόμβων, και η συνολική θύρα διέλευσης ήταν γραμμική με τον αριθμό των κόμβων. Αυτό σημαίνει ότι το HDFS επιδέχεται κλιμάκωση με τον αριθμό των κόμβων, προσφέροντας συνεχή υψηλή απόδοση και διαχείριση μεγάλων δεδομένων ακόμη και σε πολύ μεγάλες υπολογιστικές υποδομές.

3.2.6 Automated Forensic Tool – Σύστημα Υποστήριξης Εγκληματολογικής Ανάλυσης

Το Automated Forensic Tool (AFT) ενσωματώνεται στην αρχιτεκτονική ως το βασικό σύστημα για την υποστήριξη της εγκληματολογικής διερεύνησης περιστατικών ασφαλείας. Η ανάγκη για ένα τέτοιο εργαλείο προκύπτει από τη διαρκώς αυξανόμενη πολυπλοκότητα και όγκο των κυβερνοεπιθέσεων, ειδικά σε περιβάλλοντα SCADA, όπου οι συνέπειες μπορεί να είναι σοβαρές για τη λειτουργία κρίσιμων υποδομών.

Η αρχιτεκτονική του AFT οργανώνεται σε τέσσερα βασικά επίπεδα – συλλογής δεδομένων, ανάλυσης μέσω τεχνητής νοημοσύνης, σύνθεσης προφίλ επιθέσεων και διεπαφής χρήστη – τα οποία έχουν παρουσιαστεί αναλυτικά στην προηγούμενη ενότητα. Η αξία του έγκειται στον συνδυασμό εμπλουτισμένης πληροφορίας από γνωστές βάσεις δεδομένων (CAPEC, MITRE ATT&CK, CVE) και την αυτοματοποιημένη κατηγοριοποίηση και ιεράρχηση των συμβάντων, που επιτρέπει στο προσωπικό ασφαλείας να αποκτήσει άμεση εικόνα της φύσης μιας επίθεσης.

Η προσθήκη αυτού του εργαλείου ενισχύει σημαντικά τη δυναμική απόκρισης και τεκμηριωμένης λήψης αποφάσεων, μετατρέποντας τη διερεύνηση απειλών από μια εμπειρική διαδικασία σε μια δομημένη, συστηματική και επεκτάσιμη προσέγγιση, ιδανική για τη φύση και τις απαιτήσεις των SCADA συστημάτων.

3.2.7 Σύνοψη των Δομικών Επιλογών

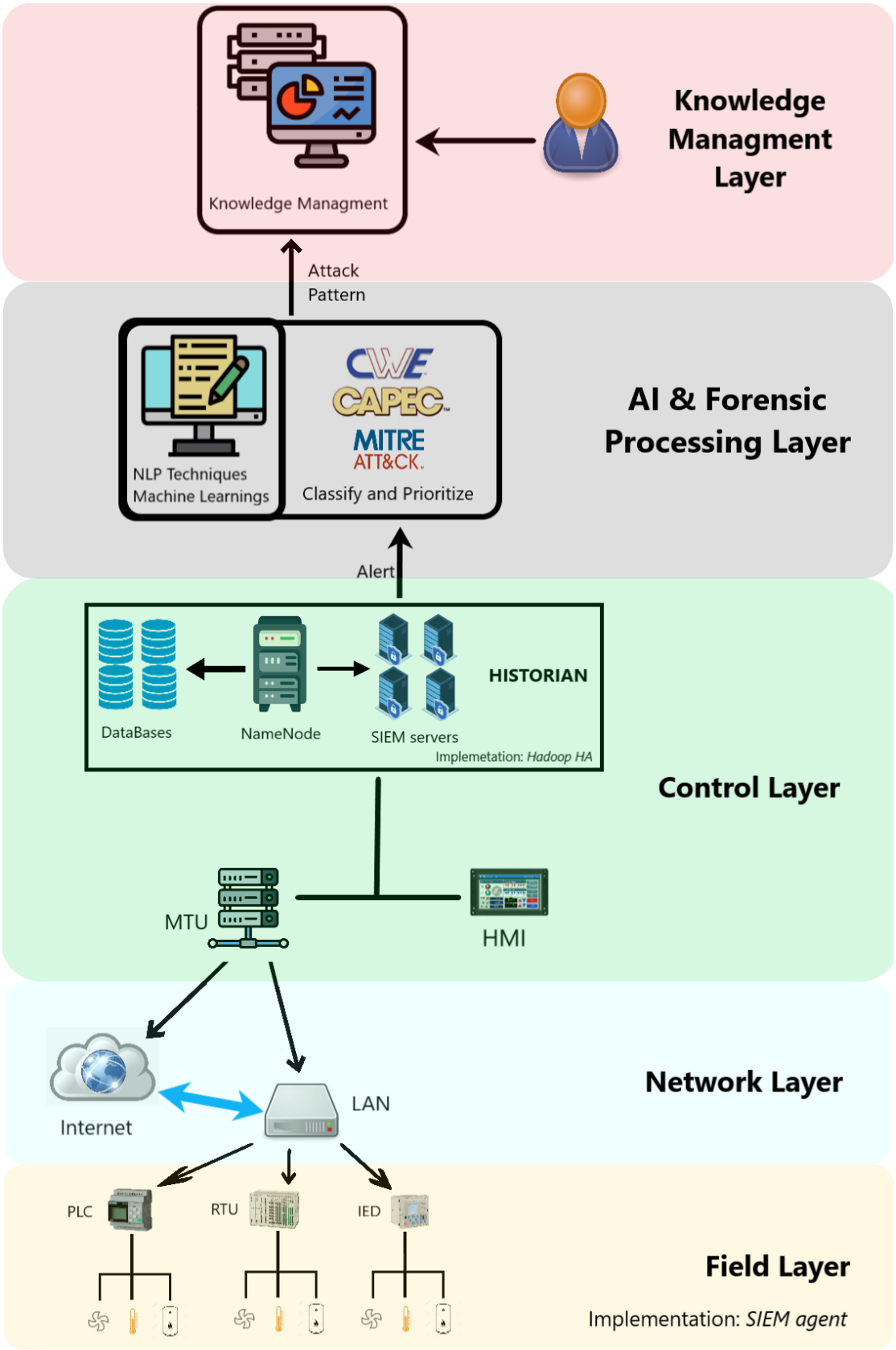
Η προτεινόμενη αρχιτεκτονική στηρίζεται σε ένα σύνολο από στοχευμένες τεχνολογικές επιλογές, οι οποίες επιλέχθηκαν με βάση τις ανάγκες ενός σύγχρονου SCADA περιβάλλοντος που απαιτεί ανθεκτικότητα, ταχύτητα απόκρισης και υψηλή παρατηρησιμότητα. Η ανάλυση των επιμέρους στοιχείων ανέδειξε τον ρόλο που διαδραματίζουν τα διαφορετικά υποσυστήματα:

- Οι **συσκευές πεδίου** (RTUs, PLCs, IEDs) αποτελούν την πηγή όλων των δεδομένων και το ευαίσθητο σημείο πρώτης επαφής με το σύστημα, καθιστώντας κρίσιμη την αξιοπιστία τους.
- Το **κεντρικό σύστημα ελέγχου** (MTU, HMI, Historian) λειτουργεί ως κόμβος συγκέντρωσης και επεξεργασίας πληροφορίας, υποστηρίζοντας την παρακολούθηση και τον έλεγχο της κατάστασης του συστήματος.
- Το **δίκτυο επικοινωνίας** διασφαλίζει την αδιάλειπτη ροή πληροφοριών, αν και απαιτεί ενισχυμένες πρακτικές ασφαλείας λόγω της ενσωματωμένης τρωτότητας των βιομηχανικών πρωτοκόλλων.
- Το **SIEM εργαλείο Wazuh** προσφέρει σε πραγματικό χρόνο δυνατότητες ανίχνευσης και αντίδρασης σε απειλές, ενισχύοντας τη δυνατότητα παρακολούθησης και συμμόρφωσης.
- Το **HDFS** επιλέχθηκε για την αξιόπιστη αποθήκευση και ανάλυση μεγάλων ποσοτήτων δεδομένων, προσφέροντας κλιμάκωση και σταθερή απόδοση.
- Τέλος, το **Automated Forensic Tool** εισάγει έναν μηχανισμό υποβοηθούμενης εγκληματολογικής ανάλυσης, δίνοντας στις ομάδες ασφαλείας τη δυνατότητα να κατανοούν καλύτερα, να κατηγοριοποιούν και να αποτρέπουν εξελιγμένες επιθέσεις.

Η συνολική συνδυαστική χρήση αυτών των στοιχείων οδηγεί σε μια συνεκτική, ευέλικτη και επεκτάσιμη αρχιτεκτονική, ικανή να ανταποκριθεί στις απαιτήσεις προστασίας ενός σύγχρονου SCADA περιβάλλοντος.

3.3 Περιγραφή και Δομή αρχιτεκτονικής

Η προτεινόμενη αρχιτεκτονική στοχεύει στη βελτίωση της ασφάλειας βιομηχανικών συστημάτων SCADA μέσω κατανεμημένης επεξεργασίας SIEM, ενσωμάτωσης τεχνικών AI για ανίχνευση επιθέσεων και δυναμικής διαχείρισης απειλών μέσω ενός Knowledge Management Layer. Στην Εικόνα 1, παρουσιάζεται η δομή της αρχιτεκτονικής, η οποία περιλαμβάνει τους απαραίτητους εξοπλισμούς για την λειτουργία ενός εργοστασίου, όπως αισθητήρες, κινητήρες, θερμόμετρα κτλ. Παρακάτω αναλύονται από κάτω προς τα πάνω τα επίπεδα.



Εικόνα 3.3-i: Δομή της προτεινόμενης αρχιτεκτονικής

3.3.1 Field Layer: Συλλογή και Τοπική Ανάλυση

Οι συσκευές πεδίου (RTUs, PLCs, IEDs) είναι υπεύθυνες για την άμεση αλληλεπίδραση με τον βιομηχανικό εξοπλισμό – όπως αισθητήρες θερμοκρασίας, πίεσης, στάθμης, αλλά και ενεργοποιητές ή μεταγωγείς – παρακολουθώντας συνεχώς κρίσιμες παραμέτρους λειτουργίας. Καθώς αυτός ο εξοπλισμός παράγει διαρκώς μεγάλες ποσότητες δεδομένων, απαιτείται προκαταρκτική ανάλυση για την αποφυγή υπερφόρτωσης του κεντρικού συστήματος. Για τον σκοπό αυτό, εγκαθίστανται SIEM agents (Wazuh) απευθείας στις συσκευές πεδίου. Οι agents αυτοί αναλαμβάνουν την τοπική συλλογή και φιλτράρισμα των δεδομένων ασφαλείας, εντοπίζοντας ύποπτες συμπεριφορές σε πραγματικό χρόνο και αποστέλλοντας στο MTU μόνο τις σχετικές ειδοποιήσεις και συμπυκνωμένες πληροφορίες. Με τον τρόπο αυτό διασφαλίζεται υψηλότερη αποδοτικότητα, ελαχιστοποιείται ο φόρτος δικτύου και αυξάνεται η ακρίβεια της ανίχνευσης απειλών στο πιο ευάλωτο επίπεδο της υποδομής. Επίσης, οι συσκευές πεδίου είναι συχνά πιο ευάλωτες σε επιθέσεις στον κυβερνοχώρο λόγω της περιορισμένης υπολογιστικής ισχύος και των χαρακτηριστικών ασφαλείας τους.

Σε ένα εναλλακτικό σενάριο, θα μπορούσε να επιλεγεί η εγκατάσταση SIEM agent απευθείας στο MTU, ώστε να υπάρχει κεντρική διαχείριση των συμβάντων ασφαλείας και μείωση του συνολικού κόστους εγκατάστασης. Ωστόσο, αυτή η προσέγγιση απορρίπτεται, καθώς περιορίζει την ορατότητα σε επίπεδο συσκευών πεδίου και μειώνει την ακρίβεια στην ανίχνευση απειλών τοπικά. Παράλληλα, η συγκέντρωση όλων των δεδομένων στο MTU θα οδηγούσε σε υπερφόρτωση του συστήματος, επιβαρύνοντας την απόδοση και καθυστερώντας την απόκριση σε κρίσιμα περιστατικά.

3.3.2 Network Layer: Επικοινωνία και Ασφάλεια

Το δίκτυο επιτρέπει τη ροή δεδομένων μεταξύ πεδίου και MTU μέσω βιομηχανικών πρωτοκόλλων (Modbus, DNP3). Η ασφάλεια ενισχύεται με firewall και πολιτικές για έλεγχο πρόσβασης και κρυπτογράφηση μεταδιδόμενων δεδομένων. Παρότι η εργασία δεν εστιάζει στην ασφάλεια του δικτύου, αναγνωρίζεται ως κρίσιμος παράγοντας.

3.3.3 Control Layer: Συγκέντρωση και Διαχείριση Δεδομένων

Μετά από ανάλυση και επεξεργασία των δεδομένων στις συσκευές πεδίου από τους SIEM agent, το MTU συλλέγει και μοιράζει τις πληροφορίες στο Historian και στο HMI (μετά από αίτημα του χρήστη). Ο Historian στηρίζεται στο HDFS με δυνατότητα High Availability (HA), διασφαλίζοντας τη συνεχή προσβασιμότητα σε περίπτωση σφάλματος. Ο Historian είναι κατανεμημένος ως εξής:

- Βάσεις δεδομένων για λειτουργικά δεδομένα.
- SIEM Servers για την αποθήκευση και επεξεργασία των δεδομένων ασφαλείας.
- 2 NameNodes(active και passive) για τη διαχείριση της κατανεμημένης αποθήκευσης.

Η εγκατάσταση SIEM servers στον Historian επιτρέπει την κεντρική αλλά κατανεμημένη ανάλυση των δεδομένων ασφαλείας. Τα δεδομένα που προέρχονται από τις συσκευές πεδίου, μέσω του MTU, μπορούν να αναλυθούν αποτελεσματικά χωρίς να υπερφορτώνεται το κεντρικό σύστημα.

Οι λόγοι επιλογής κατανεμημένη αρχιτεκτονικής SIEM servers είναι οι εξής:

- Επεκτασιμότητα: Μια κατανεμημένη αρχιτεκτονική SIEM επιτρέπει μεγαλύτερη επεκτασιμότητα. Καθώς το δίκτυο μεγαλώνει, μπορούν να προστεθούν επιπλέον διακομιστές (servers) SIEM για να χειριστούν την αυξημένη κίνηση και τον όγκο δεδομένων.
- Ανοχή σφαλμάτων: Μια κατανεμημένη αρχιτεκτονική SIEM μπορεί να είναι πιο ανεκτική σε σφάλματα από μια αρχιτεκτονική κεντρικού server. Εάν ένας server αποτύχει, οι άλλοι μπορούν να συνεχίσουν να λειτουργούν χωρίς διακοπή.
- Ανθεκτικότητα: Μια κατανεμημένη αρχιτεκτονική μπορεί να βελτιώσει την ανθεκτικότητα σε επιθέσεις στον κυβερνοχώρο. Εάν ένας εισβολέας αποκτήσει πρόσβαση σε έναν server SIEM, ενδέχεται να μην έχει πρόσβαση στους άλλους, μειώνοντας τον κίνδυνο μιας επιτυχημένης επίθεσης. Από την άλλη αν επιτεθεί σε έναν κεντρικό server θα υπάρξουν σοβαρές συνέπειες για την εταιρεία.
- Απόδοση: είναι δυνατό να επιτευχθεί καλύτερη απόδοση κατανέμοντας το φόρτο εργασίας σε πολλούς servers. Αυτό μπορεί να μειώσει την πιθανότητα προβλημάτων απόδοσης ή συμφόρησης που μπορεί να προκύψει σε μια αρχιτεκτονική κεντρικού server.

Αυτός ο σχεδιασμός ενισχύει την ικανότητα ανίχνευσης και απόκρισης σε πραγματικό χρόνο, μειώνοντας ταυτόχρονα τον κίνδυνο συμφόρησης και αυξάνοντας την ανθεκτικότητα του συστήματος.

3.3.4 AI & Forensic Processing Layer: Ευφυής Ανάλυση και Αυτοματοποιημένη Διερεύνηση

Το AI & Forensic Processing Layer αποτελεί τον πυρήνα της ευφυούς επεξεργασίας των συμβάντων ασφαλείας. Αμέσως μετά τη δημιουργία ενός alert από τους SIEM servers, το συμβάν προωθείται στο Automated Forensic Tool, το οποίο αποτελείται από τέσσερα διακριτά επίπεδα λειτουργίας. Το **Data Collector Layer** είναι υπεύθυνο για τη συλλογή πληροφοριών από διάφορες πηγές του συστήματος, όπως τα alerts των SIEM agents, τα δεδομένα του MTU και τις βάσεις δεδομένων, δημιουργώντας έτσι μια αρχική αναφορά για κάθε συμβάν ασφαλείας. Στη συνέχεια, το **Artificial Intelligence (AI) Layer** εφαρμόζει τεχνικές μηχανικής μάθησης και επεξεργασίας φυσικής γλώσσας, όπως clustering και TF-IDF, με στόχο την ανίχνευση και συσχέτιση επαναλαμβανόμενων μοτίβων επιθέσεων με δεδομένα από γνωστές βιβλιοθήκες όπως οι CAPEC, CWE και MITRE ATT&CK. Το **Forensic Intelligence Layer** αξιοποιεί τα εμπλουτισμένα αυτά δεδομένα για να συνθέσει ένα πλήρες προφίλ της επίθεσης, περιλαμβάνοντας πληροφορίες για τον πιθανό δράστη, τις τεχνικές που χρησιμοποιήθηκαν, τις σχετικές ευπάθειες, καθώς και τρόπους αντιμετώπισης. Τέλος, τα αποτελέσματα αποστέλλονται στο Knowledge Management Layer, όπου παρουσιάζονται εύχρηστα στον χρήστη.

Η συνεισφορά αυτού του επιπέδου στην αρχιτεκτονική είναι καθοριστική και εκδηλώνεται σε δύο βασικούς άξονες:

1. Ενισχύει προληπτικά την ασφάλεια του συστήματος, αξιοποιώντας τα εμπλουτισμένα δεδομένα και τα μοτίβα επιθέσεων για την αναγνώριση και πρόβλεψη πιθανών μελλοντικών απειλών. Αυτό δίνει τη δυνατότητα στο σύστημα να λειτουργεί με αυξημένο επίπεδο ετοιμότητας, εντοπίζοντας πρόδρομες ενδείξεις και περιορίζοντας τον χρόνο απόκρισης.
2. Συμβάλλει στην επιχειρησιακή τεκμηρίωση και υποστήριξη των αναλυτών κυβερνοασφάλειας, προσφέροντας οργανωμένη και πλούσια πληροφόρηση για τη φύση κάθε περιστατικού. Οι συσχετίσεις που προκύπτουν από το

επίπεδο αυτό, σε συνδυασμό με την κατηγοριοποίηση των κινδύνων, επιτρέπουν πιο στοχευμένες ενέργειες απόκρισης, αναδρομική ανάλυση, αλλά και συνεχή βελτίωση των πολιτικών ασφαλείας.

3.3.5 Knowledge Management Layer: Συγκέντρωση Πληροφοριών συμβάντων ασφαλείας

Το Knowledge Management Layer λειτουργεί ως το τελικό επίπεδο της αρχιτεκτονικής, παρέχοντας μια ολοκληρωμένη εικόνα των απειλών, της προέλευσής τους και των ενδεδειγμένων ενεργειών απόκρισης. Το επίπεδο αυτό συγκεντρώνει και οργανώνει την παραγόμενη γνώση από όλα τα προηγούμενα στάδια – SIEM, AI και Forensic Tool – και την παρουσιάζει στον αναλυτή μέσα από μια εύχρηστη διεπαφή.

Αρχικά, συγκεντρώνει τα εμπλουτισμένα δεδομένα από τις επιθέσεις, τα οποία περιλαμβάνουν μοτίβα επίθεσης, τρωτά σημεία, τεχνικές που χρησιμοποιήθηκαν, καθώς και την κρισιμότητα κάθε συμβάντος. Μέσα από αυτή τη διαδικασία επιτυγχάνεται η επαναχρησιμοποίηση της γνώσης: κάθε νέο συμβάν μπορεί να συσχετιστεί με παλαιότερες επιθέσεις, παρέχοντας στον αναλυτή συγκριτικά στοιχεία, ιστορικό, καθώς και τις αποδοτικότερες μεθόδους αντιμετώπισής του. Επιπλέον, το επίπεδο αυτό ενισχύει την υποστήριξη λήψης αποφάσεων, προσφέροντας καθοδήγηση με βάση δοκιμασμένες πρακτικές που εφαρμόστηκαν επιτυχώς στο παρελθόν. Ο χρήστης έχει πρόσβαση σε οργανωμένες πληροφορίες όπως: ποιες ενέργειες λειτούργησαν, ποια ήταν η αντίδραση του συστήματος, τι προτείνεται ως βέλτιστη απόκριση.

Η σχεδίαση του Knowledge Management Layer λαμβάνει υπόψη τις απαιτήσεις ψηφιακής εγκληματολογικής διερεύνησης. Όλα τα κρίσιμα δεδομένα ενός συμβάντος (π.χ. αρχεία καταγραφής, προφίλ επίθεσης) αποθηκεύονται σε αυθεντική μορφή με χρονική σήμανση και μηχανισμούς διασφάλισης ακεραιότητας. Με αυτόν τον τρόπο, διατηρείται η δυνατότητα επαναληπτικής ανάλυσης, ιχνηλασιμότητας των ενεργειών και δημιουργίας αποδεκτών αποδεικτικών στοιχείων για σκοπούς ψηφιακής εγκληματολογικής διερεύνησης ή μελλοντικής αξιοποίησης από τα εργαλεία ανάλυσης.

Σε περιπτώσεις κρίσιμων περιστατικών, το Knowledge Management Layer δεν περιορίζεται μόνο στην παροχή πληροφοριών, αλλά λειτουργεί και ως μηχανισμός

ενεργοποίησης απόκρισης. Με βάση προκαθορισμένους κανόνες, μπορεί να ειδοποιήσει αυτόματα τις αρμόδιες ομάδες και να δρομολογήσει επιλεγμένες ενέργειες αποτροπής ή περιορισμού του περιστατικού.

Το Knowledge Management Layer δεν αποτελεί απλώς ένα υποστηρικτικό εργαλείο, αλλά έναν δυναμικό μηχανισμό πρόληψης, τεκμηρίωσης και στρατηγικής ενίσχυσης της ασφάλειας στα SCADA συστήματα.

3.4 Σενάριο Χρήσης: Ανίχνευση και Αντιμετώπιση Κυβερνοεπιθέσεων

Παρακάτω παρατίθεται ένα ενδεικτικό σενάριο χρήσης, το οποίο αποσκοπεί στην πρακτική αποτύπωση της λειτουργίας της προτεινόμενης αρχιτεκτονικής σε συνθήκες μιας κυβερνοεπίθεσης. Μέσα από τη διαδοχική περιγραφή των βημάτων, αναδεικνύεται ο τρόπος με τον οποίο τα επιμέρους υποσυστήματα συνεργάζονται για την ανίχνευση, ανάλυση, απόκριση και τεκμηρίωση ενός περιστατικού ασφαλείας σε περιβάλλον SCADA.

Βήμα 1 – Ανίχνευση Ανωμαλίας από Πολλαπλούς SIEM Agents

Κατά τη διάρκεια της λειτουργίας, δύο διαφορετικές συσκευές πεδίου (RTU και PLC) αρχίζουν να εμφανίζουν 2 ασυνήθιστες δραστηριότητες. Πρώτον, η RTU λαμβάνει μια εντολή απενεργοποίησης αισθητήρα που δεν έχει προέλθει από το MTU. Δεύτερον, το PLC καταγράφει απότομη μεταβολή στη ροή πίεσης, η οποία δε συνάδει με προηγούμενα πρότυπα λειτουργίας.

Και οι δύο SIEM agents εκτελούν τοπική προκαταρκτική ανάλυση, εφαρμόζουν κανόνες εντοπισμού (rules) και δημιουργούν alerts με συσχετισμένα logs και εμπλουτισμένες μεταβλητές (metadata) όπως timestamp, IP πηγής, ID εντολής. Τα alerts αποστέλλονται ταυτόχρονα στον SIEM Server του Historian με χαρακτηριστικά χρονικής εγγύτητας, γεγονός που ενεργοποιεί μηχανισμό συσχέτισης συμβάντων.

Βήμα 2 – Συνδυασμένη Επεξεργασία στο Control Layer

Το MTU, έχοντας λάβει λάβει δεδομένα alerts, τα επεξεργάζεται μαζί με δεδομένα λειτουργικής δραστηριότητας άλλων συσκευών πεδίου προκειμένου να διασταυρώσει αν πρόκειται για μεμονωμένο περιστατικό ή συντονισμένη επίθεση. Αν και το HMI

παραμένει διαθέσιμο για εποπτεία, σε αυτό το στάδιο δεν εμπλέκεται ενεργά. Το MTU Προωθεί τα εμπλουτισμένα alerts και τα λειτουργικά δεδομένα στον NameNode του Historian, ο οποίος μέσω του HDFS High Availability καθοδηγεί τη διανομή τους προς:

- SIEM Servers, για περαιτέρω συσχέτιση και ανάλυση κινδύνου,
- Operational Databases, για τη διατήρηση πλήρους ιστορικού λειτουργίας.

Βήμα 3 – Ανάλυση και Συσχέτιση στο AI & Forensic Layer

Τα δεδομένα που συλλέχθηκαν και αποθηκεύτηκαν από τους SIEM servers στο Historian, μεταφέρονται στο Automated Forensic Tool για περαιτέρω ανάλυση. Το εργαλείο ενεργοποιείται αυτόματα από κάθε νέο alert ή συνδυασμό alerts που ξεπερνά συγκεκριμένα προκαθορισμένα όρια κινδύνου.

Στο Data Collector Layer, συγκεντρώνονται πληροφορίες από τα SIEM alerts, καθώς και επιπρόσθετα δεδομένα από τις Operational Databases (όπως προηγούμενες καταγραφές του ίδιου εξοπλισμού). Το AI Layer ενεργοποιείται και εφαρμόζει τεχνικές clustering και TF-IDF για να αναγνωρίσει εάν η συμπεριφορά της απειλής αντιστοιχεί σε γνωστό μοτίβο, ή αποτελεί νέο τύπο επίθεσης. Η πληροφορία εμπλουτίζεται με δεδομένα από βάσεις όπως MITRE ATT&CK, CAPEC και CWE, ώστε να ενισχυθεί το πλαίσιο κατανόησης. Το Forensic Intelligence Layer στη συνέχεια δημιουργεί ένα αναλυτικό προφίλ της απειλής, συμπεριλαμβανομένων πιθανών στόχων, μεθόδων εκμετάλλευσης και βέλτιστων πρακτικών απόκρισης. Η έξοδος του εργαλείου προωθείται στο Knowledge Management Layer, όπου θα διατηρηθεί για μελλοντική αξιοποίηση και προβολή.

Βήμα 4 – Δράση και Απόκριση μέσω Knowledge Management Layer

Μόλις ολοκληρωθεί η ανάλυση και δημιουργηθεί το προφίλ της απειλής, οι πληροφορίες αποθηκεύονται και ενεργοποιούνται στο Knowledge Management Layer. Το επίπεδο αυτό λειτουργεί ως κόμβος λήψης αποφάσεων και επιχειρησιακής υποστήριξης για τον αναλυτή ασφάλειας.

Οι σχετικές εγγραφές εμφανίζονται μέσω του GUI, εμπλουτισμένες με προτάσεις αντιμετώπισης, επίπεδα σοβαρότητας και συσχετισμούς με παλαιότερα περιστατικά. Ο αναλυτής μπορεί να εξετάσει:

- Συσχετισμένα incidents από το παρελθόν,

- Τάσεις επανάληψης, εάν η επίθεση εμφανίζεται ως μέρος ενός μοτίβου,
- Συστάσεις απόκρισης, όπως αποκλεισμός IP, τροποποίηση πολιτικών firewall ή ενημέρωση κανόνων SIEM,
- Χρονικό ιστορικό και context γύρω από τη δραστηριότητα του εξοπλισμού.

Σε περίπτωση κρίσιμου περιστατικού, το Knowledge Layer ενεργοποιεί αυτόματα μηχανισμούς ειδοποίησης προς τις αρμόδιες ομάδες (π.χ. SOC, IT Admins), ενώ παράλληλα μπορεί να επιβάλει αυτόματες ενέργειες μέσω προδιαγεγραμμένων κανόνων (π.χ. απομόνωση δικτυακής συσκευής, τροποποίηση ACL). Το αποτέλεσμα της ανάλυσης και της απόκρισης ενσωματώνεται στην υπάρχουσα γνώση του συστήματος, ενισχύοντας τη δυνατότητα προβλεπτικής ασφάλειας και αυτοματοποιημένης απόφασης σε μελλοντικά περιστατικά.

Επιπρόσθετα, όλα τα σχετικά δεδομένα που αφορούν το περιστατικό, περιλαμβανομένων των αρχικών καταγραφών και των ενδιάμεσων αποτελεσμάτων ανάλυσης, αποθηκεύονται αυτούσια με χρονική σήμανση και μηχανισμούς διατήρησης ακεραιότητας. Με τον τρόπο αυτό διασφαλίζεται δυνατότητα ανασύνθεσης του περιστατικού σε μεταγενέστερο χρόνο και τεκμηριωμένη υποστήριξη ψηφιακής εγκληματολογικής διερεύνησης, όταν απαιτείται.

3.5 Καινοτομία της Προτεινόμενης Αρχιτεκτονικής

Η προτεινόμενη αρχιτεκτονική διαφοροποιείται από υπάρχουσες προσεγγίσεις καθώς συνδυάζει, για πρώτη φορά σε περιβάλλον SCADA, κατανεμημένη ανάλυση συμβάντων, σύγχρονα εργαλεία ανίχνευσης και αποθήκευσης, τεχνικές τεχνητής νοημοσύνης και σύστημα διαχείρισης γνώσης σε ενιαία, συνεκτική υποδομή. Η κύρια καινοτομία εντοπίζεται στη διασύνδεση τριών κρίσιμων εργαλείων:

- SIEM (Wazuh): ένα ελαφρύ εργαλείο ανοιχτού κώδικα (open-source) τοποθετημένο απευθείας στις συσκευές πεδίου που επιτρέπει την τοπική ανάλυση συμβάντων ασφαλείας πριν τα δεδομένα μεταδοθούν στο κεντρικό σύστημα. Επιλέχθηκε, λόγω της ευκολίας προσαρμογής του σε διαφορετικές υποδομές και της συμβατότητάς του με συσκευές περιορισμένων δυνατοτήτων, όπως αυτές που συναντώνται σε περιβάλλοντα SCADA.
- HDFS High Availability: Το HDFS προσφέρει υψηλή απόδοση ανάγνωσης/εγγραφής, κλιμάκωση με βάση τον αριθμό κόμβων και αντοχή σε

σφάλματα. Η αρχιτεκτονική HA διασφαλίζει συνέχιση λειτουργίας ακόμη και σε περίπτωση αστοχίας NameNode, ενώ ο διαχωρισμός μεταξύ operational databases και SIEM servers επιτρέπει την παράλληλη ανάλυση λειτουργικών και ασφαλιστικών δεδομένων χωρίς σύγκρουση ενδιαφερόντων πόρων.

- Automated Forensic Tool: Ενσωματώνει τεχνολογίες AI και NLP, υποστηρίζοντας αυτόματο εμπλουτισμό των alerts και δημιουργία προφίλ επίθεσης με βάση γνωστά μοτίβα. Επιλέχθηκε επειδή παρέχει συνδυαστική ανάλυση μεταξύ γεγονότων, αξιοποιεί εξωτερικές βάσεις δεδομένων απειλών (όπως CAPEC, CWE, MITRE ATT&CK) και προσφέρει υποστήριξη λήψης απόφασης για τον αναλυτή με βάση ιστορικά πρότυπα. Έτσι, ενισχύει τη δυνατότητα ανάλυσης και πρόβλεψης, αξιοποιώντας κάθε περιστατικό ως βάση για τη συνεχή βελτίωση της αμυντικής στρατηγικής του συστήματος.

Η αρχιτεκτονική επιτυγχάνει υψηλή επεκτασιμότητα και αντοχή σε σφάλματα, αποφεύγοντας τη συγκέντρωση της ανάλυσης σε έναν μόνο κόμβο. Παράλληλα, υποστηρίζει πρόβλεψη επιθέσεων και αξιοποίηση προηγούμενων συμβάντων, καθιστώντας την ιδανική για σύγχρονα SCADA περιβάλλοντα που απαιτούν ταχύτατη αντίδραση και τεκμηριωμένη λήψη αποφάσεων.

3.6 Σύγκριση Υφιστάμενων Αρχιτεκτονικών Κυβερνοασφάλειας σε SCADA

Στο πεδίο των συστημάτων SCADA, έχουν παρουσιαστεί αρχιτεκτονικές κυβερνοασφάλειας που επιχειρούν να συνδυάσουν επιμέρους λειτουργίες. Ωστόσο, οι περισσότερες από αυτές εστιάζουν σε συγκεκριμένες μόνο πτυχές της ασφάλειας, χωρίς να διαμορφώνουν μια συνεκτική, ολιστική προσέγγιση προσαρμοσμένη στις ιδιαιτερότητες των SCADA υποδομών.

Οι προσεγγίσεις αυτές συνήθως κινούνται σε δύο κύριες κατευθύνσεις:

1. **Προσεγγίσεις επικεντρωμένες στην υποδομή και τον εξοπλισμό (hardware-centric):** Περιλαμβάνουν λεπτομερή περιγραφή της αρχιτεκτονικής των βιομηχανικών στοιχείων του SCADA συστήματος, όπως οι RTUs, PLCs και HMIs. Δίνουν έμφαση στην προστασία των φυσικών και λειτουργικών συσκευών από απειλές, με στόχο την ενίσχυση της αξιοπιστίας και της ασφάλειας του ίδιου του εξοπλισμού. (Ανάλυση στο Κεφάλαιο 3.6.1)

2. **Προσεγγίσεις επικεντρωμένες στη διαχείριση δεδομένων και την ανάλυση συμβάντων (software-centric):** Εστιάζουν στη συλλογή, επεξεργασία και συσχέτιση συμβάντων ασφάλειας αξιοποιώντας:
    - χρήση εργαλείων SIEM για συλλογή και συσχέτιση συμβάντων ασφαλείας,
    - αξιοποίηση τεχνικών τεχνητής νοημοσύνης για ανίχνευση ή ταξινόμηση επιθέσεων,
    - υποστήριξη ψηφιακής εγκληματολογικής διερεύνησης και συλλογής αποδεικτικών στοιχείων,
    - ενσωμάτωση πληροφοριών απειλών και δυναμική συσχέτιση,
    - τεχνικές εμπλουτισμού των συναγερμών από γνωστές βάσεις δεδομένων (CAPEC, MITER ATT&CK και CVE).

3.6.1 Σύγκριση φυσικών υποδομών SCADA

Η αξιολόγηση της υποδομής SCADA αποτελεί κρίσιμο πεδίο ανάλυσης, καθώς σχετίζεται άμεσα με τη λειτουργικότητα, την απόδοση και την ανθεκτικότητα των βιομηχανικών συστημάτων. Στο πλαίσιο αυτό, εξετάζονται διαφορετικές αρχιτεκτονικές που είτε βασίζονται σε παραδοσιακά πρότυπα σχεδίασης είτε ενσωματώνουν σύγχρονες τεχνολογίες, όπως το edge computing και το Internet of Things (IoT). Η σύγκριση επικεντρώνεται κυρίως στα φυσικά υποσυστήματα κάθε αρχιτεκτονικής, τον τρόπο με τον οποίο διαχειρίζονται τη ροή δεδομένων από και προς το πεδίο, καθώς και την αποδοτικότητα που επιτυγχάνουν σε συνθήκες λειτουργίας. Μέσω της ανάλυσης αυτών των παραμέτρων, αναδεικνύονται τα τεχνικά πλεονεκτήματα και οι περιορισμοί κάθε προσέγγισης.

Για την ενδεικτική ανάλυση που ακολουθεί, επιλέχθηκαν τρεις επιστημονικές εργασίες με βάση την επικαιρότητά τους, το εύρος των θεμάτων που καλύπτουν (όπως αρχιτεκτονική, ασφάλεια και σύγχρονες τεχνολογίες), καθώς και τη συνάφεια με τις βασικές διαστάσεις της παρούσας εργασίας. Οι εργασίες αυτές κρίθηκαν ως επαρκώς αντιπροσωπευτικές, καθώς παρέχουν διαφορετικές αλλά συμπληρωματικές οπτικές πάνω στη δομή και τις προκλήσεις των σύγχρονων SCADA συστημάτων.

3.6.1.1 Αρχιτεκτονική Άρθρου [40] – Ενισχυμένη SCADA με IoT και Fog Υποστήριξη

Η αρχιτεκτονική που περιγράφεται στο άρθρο [40] στοχεύει στην ενίσχυση της ασφάλειας και της λειτουργικότητας υφιστάμενων SCADA υποδομών, αξιοποιώντας τεχνολογίες Διαδικτύου των Πραγμάτων (Internet of Things – IoT), υπολογιστικού νέφους (cloud computing) και υπολογιστικής ομίχλης (fog computing). Είναι μια ιεραρχική αρχιτεκτονική που περιλαμβάνει το επίπεδο πεδίου (PLC, RTU, IED), το επίπεδο ελέγχου (MTU) και επίπεδο εποπτείας και αποθήκευσης. Το επίπεδο του πεδίου εμπλουτίζεται με έξυπνους αισθητήρες, διαμεσολαβητές (IoT gateways) και κόμβους περιφερειακής επεξεργασίας δεδομένων (Edge nodes). Οι επεκτάσεις αυτές επιτρέπουν την τοπική προεπεξεργασία, την πιο αποτελεσματική συλλογή και ανάλυση πληροφοριών, καθώς και την ενσωμάτωση μηχανισμών ασφάλειας.

Πλεόνεκτήματα

- Ο παραδοσιακός εξοπλισμός ενισχύεται με αισθητήρες IoT και gateway συσκευές χωρίς πλήρη αντικατάσταση του. Με τον τρόπο αυτό, επιτυγχάνεται ουσιαστική αναβάθμιση της λειτουργικότητας και της αποδοτικότητας των υπαρχουσών βιομηχανικών υποδομών, με περιορισμένο κόστος και χωρίς σημαντικές επεμβάσεις στο υφιστάμενο σύστημα.
- Μειώνει τη ροή δεδομένων προς τα κεντρικά συστήματα χρησιμοποιώντας fog computing για προεπεξεργασία δεδομένων κοντά στο πεδίο.
- Μπορεί να επεκταθεί με νέα σημεία συλλογής χωρίς αναδιάρθρωση των υποδομών.
- Οι RTU ή gateways μπορούν να εκτελούν προκαθορισμένες ενέργειες χωρίς να απαιτείται κεντρική εντολή, με την υποστήριξη edge αυτονομίας μειώνοντας τον χρόνο απόκρισης.

Μειονεκτήματα

- Η ταυτόχρονη χρήση παραδοσιακών στοιχείων SCADA, αισθητήρων IoT, gateways, καθώς και υποδομών fog ή cloud computing, απαιτεί εξειδικευμένο συντονισμό μεταξύ διαφορετικών τεχνολογικών επιπέδων. Αυτό δημιουργεί επιπλέον απαιτήσεις τόσο σε τεχνική υποστήριξη όσο και σε διαλειτουργικότητα των συστημάτων.

- Παρά τη δυνατότητα αποστολής δεδομένων σε υποδομές cloud ή historian, η αποκεντρωμένη φύση της αρχιτεκτονικής περιορίζει σε ορισμένες περιπτώσεις την ενιαία και έγκαιρη ενοποίηση των πληροφοριών. Εφόσον η ανάλυση και απόκριση πραγματοποιούνται τοπικά σε edge κόμβους, χωρίς υποχρεωτική αποστολή όλων των δεδομένων ή λεπτομερών ιχνών στο κεντρικό σύστημα, καθίσταται δυσκολότερη η πλήρης εγκληματολογική αξιολόγηση.
- Ακόμη και αν οι πλατφόρμες υπολογιστικού νέφους είναι τεχνικά αξιόπιστες, η χρήση τους συνεπάγεται απώλεια πλήρους ελέγχου από την πλευρά του οργανισμού. Η εξάρτηση από τρίτους παρόχους περιορίζει τη δυνατότητα άμεσης επέμβασης σε κρίσιμες συνθήκες, ενώ ενδέχεται να εισάγει κινδύνους σχετικούς με τη διαθεσιμότητα, την κυριότητα των δεδομένων ή τη συμμόρφωση με θεσμικά και νομικά πλαίσια, παράγοντες ιδιαίτερα σημαντικούς σε βιομηχανικά περιβάλλοντα υψηλής κρισιμότητας.

3.6.1.2 Αρχιτεκτονική Άρθρου [41] – IoT-SCADA Σύστημα για Διαχείριση Δικτύου Ηλεκτρικής Ενέργειας

Η αρχιτεκτονική που παρουσιάζεται στο άρθρο [41] φέρει σημαντικές ομοιότητες με την προσέγγιση του άρθρου [40], καθώς βασίζεται σε μια υφιστάμενη SCADA υποδομή, την οποία εμπλουτίζει με τεχνολογίες IoT, fog υποδομές και δυνατότητες cloud επεξεργασίας. Η βασική διαφοροποίηση εντοπίζεται στο γεγονός ότι η προτεινόμενη λύση εφαρμόζεται στο πεδίο της ηλεκτρικής ενέργειας και υιοθετεί αυστηρή διαστρωμάτωση σύμφωνα με το πρότυπο ISA-99, με ενσωμάτωση επιχειρησιακών πληροφοριακών συστημάτων, όπως ERP και GIS. Επιπλέον, δίνεται ιδιαίτερη έμφαση στη διαλειτουργικότητα και στη διασύνδεση του SCADA με άλλα λειτουργικά τμήματα του οργανισμού.

Πλεονεκτήματα

- Η συμμόρφωση με ISA-99 πρότυπα.
- Η διασύνδεση με επιχειρησιακά πληροφοριακά συστήματα, όπως τα ERP (Enterprise Resource Planning) και GIS (Geographic Information Systems), καθιστά την αρχιτεκτονική κατάλληλη για πλήρη επιχειρησιακή ενοποίηση. Τα δεδομένα που συλλέγονται από το SCADA μπορούν να αξιοποιούνται όχι μόνο

για λειτουργικό έλεγχο, αλλά και για οικονομική, διοικητική και γεωχωρική ανάλυση, ενισχύοντας τη λήψη αποφάσεων σε πραγματικό χρόνο.

- Η δομημένη χρήση fog υποδομών για προεπεξεργασία δεδομένων βοηθά στη μείωση του όγκου των μεταφερόμενων δεδομένων και στη βελτίωση της απόκρισης σε κατανεμημένες περιοχές.

Μειονεκτήματα

- Η υλοποίηση ενός πλήρως διασυνδεδεμένου οικοσυστήματος, που περιλαμβάνει αισθητήρες IoT, fog κόμβους, cloud, καθώς και διασύνδεση με τρίτα επιχειρησιακά συστήματα (όπως ERP/GIS), συνεπάγεται σημαντικό οικονομικό και τεχνικό κόστος.
- Η πολυπλοκότητα της αρχιτεκτονικής ενισχύεται από την ανάγκη συγχρονισμού πολλαπλών επιπέδων πληροφορίας, καθώς τα δεδομένα ταξιδεύουν από το πεδίο στο fog, από εκεί στο cloud, και τελικά διατίθενται σε ERP ή GIS. Η διαχείριση συγχρονισμού, καθυστερήσεων, και consistency ανάμεσα σε αυτά τα επίπεδα αποτελεί πρόκληση.

3.6.1.3 Αρχιτεκτονική Άρθρου [42] – Προηγμένη Αρχιτεκτονική SCADA για Αυτόνομη Λειτουργία σε Πεδίο Πετρελαίου και Φυσικού Αερίου

Η αρχιτεκτονική που παρουσιάζεται στο άρθρο [42] προτείνει μια ριζικά διαφοροποιημένη προσέγγιση σε σχέση με τις προηγούμενες λύσεις, βασιζόμενη στην αρχή της πλήρους αποκέντρωσης και της εγγενούς ενσωμάτωσης edge υπολογιστικών πόρων. Το σύστημα σχεδιάστηκε ειδικά για περιβάλλοντα υψηλής απαιτητικότητας, όπως γεωγραφικά κατανεμημένα πεδία πετρελαίου και φυσικού αερίου, όπου η ανάγκη για αυτονομία, χαμηλή καθυστέρηση και ενισχυμένη αξιοπιστία είναι ιδιαίτερα κρίσιμη. Η αρχιτεκτονική περιλαμβάνει έξυπνες RTU μονάδες και edge gateways με αυξημένες υπολογιστικές δυνατότητες, ικανές να εκτελούν τοπικά μοντέλα μηχανικής μάθησης, να εφαρμόζουν προγνωστικές ειδοποιήσεις και να ενεργοποιούν ελέγχους κλειστού βρόχου χωρίς την ανάγκη ενός κεντρικού ελέγχου. Επιπλέον, το κάθε edge node είναι εξοπλισμένο με δικό του ιστορικό αποθήκευσης (local historian), επιτρέποντας την καταγραφή και συγχρονισμό δεδομένων ακόμη και σε περιπτώσεις προσωρινής αποσύνδεσης από το δίκτυο. Το σύστημα ενσωματώνει ανάλυση

βασισμένη σε υπολογιστικό νέφος για μη κρίσιμες λειτουργίες, όπως η εκπαίδευση αλγορίθμων τεχνητής νοημοσύνης και η διαχείριση εξοπλισμού πεδίου.

Πλεονεκτήματα

- Η αρχιτεκτονική παρέχει εξαιρετική ανθεκτικότητα και αυτονομία, χάρη στην ενσωμάτωση έξυπνων RTUs που διαθέτουν υπολογιστική ισχύ και δυνατότητα άμεσης λήψης αποφάσεων σε επίπεδο πεδίου.
- Η προεπεξεργασία και φιλτράρισμα των δεδομένων σε επίπεδο edge ελαχιστοποιεί τη χρήση του διαθέσιμου bandwidth, μειώνει την καθυστέρηση απόκρισης και αυξάνει την αποδοτικότητα του συστήματος.
- Η χρήση ενσωματωμένων εργαλείων τεχνητής νοημοσύνης για προγνωστική συντήρηση και διαχείριση κινδύνων ενισχύει την αποτελεσματικότητα και επιτρέπει βελτιστοποίηση των πόρων με ελάχιστη ανθρώπινη παρέμβαση.
- Η κάθε υποσυστατική μονάδα (όπως η τοπική ανάλυση, η αποθήκευση, ή η τεχνητή νοημοσύνη) λειτουργεί αυτόνομα και μπορεί να ενσωματωθεί ή να αφαιρεθεί χωρίς να επηρεάζεται η συνοχή και η λειτουργία του συνολικού συστήματος.

Μειονεκτήματα

- Η έντονα αποκεντρωμένη φύση της επεξεργασίας, αν και ωφέλιμη σε επίπεδο απόκρισης, ενδέχεται να προκαλέσει προκλήσεις στην ενοποίηση δεδομένων και τη συνολική εγκληματολογική ανάλυση. Όταν η απόφαση λαμβάνεται και εκτελείται τοπικά, χωρίς πάντα να μεταφέρεται το πλήρες ιστορικό ή τα αρχικά δεδομένα προς το κέντρο, η δυνατότητα ανακατασκευής συμβάντων ασφάλειας μπορεί να περιοριστεί.
- Η υλοποίηση ενός τέτοιου συστήματος απαιτεί ακριβό και σύνθετο εξοπλισμό πεδίου, όπως RTUs με επεξεργαστικές μονάδες και edge servers με δυνατότητα τεχνητής νοημοσύνης. Το κόστος αυτών των στοιχείων, σε συνδυασμό με την ανάγκη συνεχούς συγχρονισμού και ενημέρωσης, αυξάνει τον προϋπολογισμό υλοποίησης και συντήρησης.
- Η συνολική πολυπλοκότητα διαχείρισης αυξάνεται επίσης, καθώς απαιτείται συντονισμός μεταξύ cloud, edge και τοπικών μονάδων, με αυστηρές απαιτήσεις για συγχρονισμό και ασφάλεια.

3.6.1.4 Συγκεντρωτική Αξιολόγηση Ενισχυμένων Υποδομών SCADA

Η συγκριτική αξιολόγηση των αρχιτεκτονικών αναδεικνύει διαφορετικά επίπεδα τεχνολογικής ωριμότητας, αποκέντρωσης και στρατηγικής εστίασης. Οι αρχιτεκτονικές των άρθρων [40] και [41] υιοθετούν μοντέλα IoT-ενισχυμένου SCADA, με χρήση fog υποδομών και υπολογιστικού νέφους για τη συλλογή και επεξεργασία δεδομένων. Αν και επεκτείνουν τη λειτουργικότητα των υφιστάμενων συστημάτων με νέες δυνατότητες ανάλυσης και παρακολούθησης, βασίζονται έντονα σε cloud υποδομές και διατηρούν κατανεμημένη πληροφορία, γεγονός που ενδέχεται να περιορίζει τη συνεκτική αντιμετώπιση συμβάντων ασφαλείας και τη δυνατότητα εγκληματολογικής διερεύνησης. Επιπλέον, στην περίπτωση του άρθρου [41], η ενσωμάτωση εξωτερικών πληροφοριακών συστημάτων (ERP, GIS) αυξάνει τη λειτουργική πολυπλοκότητα και απαιτεί ενισχυμένες τεχνικές γνώσεις για διαχείριση και συντήρηση.

Η αρχιτεκτονική του άρθρου [42] προτείνει ένα αποκεντρωμένο μοντέλο με ισχυρούς υπολογιστικούς κόμβους στο πεδίο που μπορούν να λάβουν τοπικά αποφάσεις και να λειτουργήσουν αυτόνομα. Παρά την υψηλή απόδοση και την ικανότητα real-time απόκρισης, η πλήρης αποκέντρωση δημιουργεί σοβαρές προκλήσεις ως προς την ενοποίηση των δεδομένων, τον συσχετισμό συμβάντων και την επανασύνθεση κρίσιμων ακολουθιών για ανάλυση ασφαλείας. Παράλληλα, η ανάγκη για εξειδικευμένο και ακριβό εξοπλισμό καθιστά τη λύση αυτή δύσκολα εφαρμόσιμη σε υφιστάμενες βιομηχανικές εγκαταστάσεις.

Η αρχιτεκτονική που προτείνεται στην παρούσα διπλωματική εργασία εστιάζει στην ενίσχυση της κυβερνοασφάλειας των SCADA συστημάτων, αξιοποιώντας ελαφριούς Wazuh agents και κατάλληλα τεχνολογικά εργαλεία, χωρίς να απαιτείται τροποποίηση ή αντικατάσταση του υπάρχοντος βιομηχανικού εξοπλισμού. Η προσέγγιση επικεντρώνεται στην παρακολούθηση, ανάλυση και συσχέτιση συμβάντων ασφαλείας, με στόχο την ενίσχυση της συνολικής ανθεκτικότητας του συστήματος. Παράλληλα, διατηρείται η αποδοτικότητα και η σταθερότητα λειτουργίας της SCADA υποδομής, καθώς η προτεινόμενη λύση λειτουργεί υποστηρικτικά και όχι παρεμβατικά ως προς τον βασικό μηχανισμό ελέγχου και αυτοματισμού.

Επιπρόσθετα, μέσω τοπικής προεπεξεργασίας των δεδομένων στους agents, περιορίζεται σημαντικά η επιβάρυνση του MTU και η ανάγκη για αποστολή

ανεπεξέργαστων πληροφοριών, χωρίς να διακυβεύεται η συνοχή της πληροφορίας. Με τον τρόπο αυτό, επιτυγχάνεται μια ισορροπημένη λύση που συνδυάζει το χαμηλό λειτουργικό κόστος, τη διατηρησιμότητα των υφιστάμενων υποδομών και την κάλυψη κρίσιμων αναγκών κυβερνοασφάλειας, οι οποίες παραμένουν μερικώς ακάλυπτες στις υπόλοιπες αρχιτεκτονικές.

3.6.2 Σύγκριση λύσεων στην διαχείριση συμβάντων ασφαλείας SCADA

Η διαχείριση συμβάντων ασφαλείας σε συστήματα SCADA αποτελεί σημαντικό παράγοντα για την προστασία κρίσιμων υποδομών από κακόβουλες ενέργειες ή δυσλειτουργίες. Λόγω της αυξανόμενης συνδεσιμότητας και πολυπλοκότητας αυτών των συστημάτων, έχουν αναπτυχθεί διάφορες λύσεις για την ανίχνευση, παρακολούθηση και απόκριση σε περιστατικά ασφαλείας. Στην ενότητα αυτή, πραγματοποιείται συγκριτική ανάλυση επιλεγμένων προσεγγίσεων, με βάση την αποδοτικότητα, την ακρίβεια, την ευκολία ενσωμάτωσης και την ανταπόκρισή τους σε πραγματικό χρόνο, προκειμένου να εντοπιστούν τα πλεονεκτήματα και οι αδυναμίες της κάθε λύσης.

Για την υποστήριξη της ανάλυσης που ακολουθεί, επιλέχθηκαν ενδεικτικές επιστημονικές εργασίες που προτείνουν ολοκληρωμένες προσεγγίσεις για την ανίχνευση, συσχέτιση και απόκριση σε κυβερνοαπειλές σε περιβάλλοντα SCADA. Οι λύσεις αυτές επιλέχθηκαν επειδή ενσωματώνουν τεχνολογικές καινοτομίες (όπως SIEM, AI, forensics, compliance) και έχουν εφαρμοστεί ή δοκιμαστεί σε κρίσιμες υποδομές, προσφέροντας ουσιαστικά παραδείγματα με πρακτική αξία.

3.6.2.1 CIPSEC [37] – Ενοποιημένο Πλαίσιο Ασφάλειας για Κρίσιμες Υποδομές

Το πρόγραμμα CIPSEC εισάγει έναν προηγμένο ενιαίο μηχανισμό ασφάλειας που ενσωματώνεται σε κρίσιμες υποδομές όπως τα συστήματα SCADA, προσφέροντας ένα συντονισμένο και ευέλικτο πλαίσιο για τη διαχείριση συμβάντων ασφαλείας και την

αντιμετώπιση κυβερνοαπειλών. Στο πλαίσιο αυτό, αξιοποιούνται τεχνολογικά μέσα αιχμής που καλύπτουν τόσο τον τομέα της πληροφορικής (IT) όσο και των λειτουργικών τεχνολογιών (OT). Εργαλεία όπως το XL-SIEM παρέχουν δυνατότητες πραγματικού χρόνου για ανίχνευση ανωμαλιών και συσχέτιση συμβάντων από ποικίλες πηγές, διασφαλίζοντας συνεχή εποπτεία του συστήματος. Παράλληλα, λύσεις αντι-κακόβουλου λογισμικού που βασίζονται σε τεχνικές μηχανικής μάθησης, αναλύουν τη συμπεριφορά του συστήματος και εντοπίζουν άγνωστες απειλές. Την ασφάλεια ενισχύουν honeypot μηχανισμοί, οι οποίοι παγιδεύουν επιθέσεις σε απομονωμένα περιβάλλοντα, συλλέγοντας κρίσιμες πληροφορίες για τη μεθοδολογία των εισβολέων.

Επιπλέον, η τεχνολογία DoSSensing επιτρέπει την ανίχνευση επιθέσεων άρνησης υπηρεσίας (DoS) σε φυσικό επίπεδο, εντοπίζοντας παρεμβολές στη ζώνη ασύρματης επικοινωνίας των αισθητήρων και των στοιχείων IoT. Το σύστημα ενσωματώνει επίσης εργαλεία για διαχείριση ταυτότητας και πρόσβασης (όπως το SecoCard), hardware security modules για την εκτέλεση κρυπτογραφικών λειτουργιών σε ασφαλές περιβάλλον, καθώς και λύσεις οπτικοποίησης εγκληματολογικών δεδομένων για την υποστήριξη της απόκρισης και της ανάλυσης περιστατικών.

Αυτή η πολυεπίπεδη προσέγγιση στη διαχείριση συμβάντων ασφαλείας και την προστασία των SCADA ενσωματώνει τεχνολογίες ανίχνευσης, πρόληψης, απόκρισης και ανάκτησης, με στόχο τη συνολική ενίσχυση της ανθεκτικότητας των υποδομών απέναντι σε σύγχρονες και εξελισσόμενες απειλές.

Πλεονεκτήματα.

- SIEM και συσχέτιση συμβάντων (XL-SIEM): Ο κεντρικός μηχανισμός XL-SIEM επιτρέπει τη συλλογή και συσχέτιση δεδομένων από ετερογενείς αισθητήρες και λογισμικά ασφαλείας, δημιουργώντας ένα ενοποιημένο περιβάλλον εποπτείας και ανάλυσης.
- Υποστήριξη ψηφιακής εγκληματολογικής διερεύνησης: Το σύστημα προσφέρει οπτικοποίηση digital forensics και δυνατότητα συλλογής δεδομένων για ανάλυση περιστατικών.
- Επιλεγμένη χρήση τεχνικών τεχνητής νοημοσύνης (AI): Αναφέρεται χρήση μηχανικής μάθησης στην πλατφόρμα Bitdefender για την ανίχνευση άγνωστων απειλών.

Μειονεκτήματα

- Το σύστημα συσχέτισης και ανάλυσης συμβάντων στο CIPSEC βασίζεται στο XL-SIEM, μια εσωτερική πλατφόρμα SIEM που αναπτύχθηκε από την εταιρεία ATOS στο πλαίσιο ερευνητικών έργων. Αν και παρέχει προηγμένες δυνατότητες συσχέτισης και ανάλυσης, δεν αποτελεί ευρέως διαθέσιμο εμπορικό προϊόν. Η λειτουργία του εξαρτάται από εξειδικευμένες επεκτάσεις (plugins) και όχι με γνωστά πρωτόκολλα προς τα υπόλοιπα υποσυστήματα της αρχιτεκτονικής. Αυτό ενδέχεται να περιορίσει την επεκτασιμότητα της αρχιτεκτονικής. Η ενσωμάτωση νέων πηγών δεδομένων ή η μετάβαση σε εναλλακτικά εργαλεία SIEM προϋποθέτει την ανάπτυξη νέων επεκτάσεων, κάτι που προσθέτει τεχνική πολυπλοκότητα και εξάρτηση από συγκεκριμένες τεχνολογικές επιλογές.
- Δεν τεκμηριώνεται η ύπαρξη μηχανισμού που να εμπλουτίζει τους συναγερμούς ασφαλείας με επιπλέον πληροφορίες ή με παλιότερα γεγονότα.
- Παρά την ύπαρξη υποδομών για διερεύνηση περιστατικών, δεν παρουσιάζεται σε βάθος η δυνατότητα αποθήκευσης των πρωτογενών δεδομένων με τρόπο που να εξασφαλίζει την ακεραιότητα, την ιχνηλασιμότητα και τη χρονική τεκμηρίωση, όπως απαιτείται για την πλήρη ετοιμότητα ψηφιακής εγκληματολογικής διερεύνησης.

3.6.2.2 IADS [38] – Πλαίσιο Ανίχνευσης Εισβολών και Ελέγχου Συμμόρφωσης για Κρίσιμες Υποδομές

Το IADS (Intrusion and Anomaly Detection System) [37] αποτελεί ένα εξελιγμένο πλαίσιο ασφάλειας για την προστασία κρίσιμων υποδομών, το οποίο ενσωματώνει μηχανισμούς ψηφιακής εγκληματολογικής διερεύνησης και κανονιστικού ελέγχου. Σε αντίθεση με άλλα συστήματα που επικεντρώνονται κυρίως στην πρόληψη και ανίχνευση, το IADS δίνει ιδιαίτερη έμφαση στη δυνατότητα μεταγενέστερης ανάλυσης περιστατικών και στην επιβεβαίωση συμμόρφωσης με πολιτικές ασφαλείας.

Η αρχιτεκτονική του συστήματος είναι σχεδιασμένη ώστε να συλλέγει και να επεξεργάζεται μεγάλους όγκους ετερογενούς πληροφορίας από διαφορετικές πηγές, όπως αρχεία καταγραφής, συμβάντα ελέγχου πρόσβασης και ροές δικτύου. Η επεξεργασία βασίζεται σε σύγχρονες τεχνικές ανάλυσης και μηχανικής μάθησης, ενώ

η ανάλυση ανωμαλιών και η παρακολούθηση συμμόρφωσης πραγματοποιούνται σε σχεδόν πραγματικό χρόνο. Το σύστημα έχει υλοποιηθεί και αξιολογηθεί στο πλαίσιο του ευρωπαϊκού έργου ATENA, χρησιμοποιώντας κατανεμημένες υποδομές και τεχνολογίες Elasticsearch.

Η λειτουργικότητα του πλαισίου υποστηρίζει τόσο την εντολή επιθέσεων πολλαπλών σταδίων όσο και τη χρονική συσχέτιση γεγονότων, προσφέροντας δυνατότητες όπως ανακατασκευή ακολουθίας γεγονότων (timeline reconstruction), δείκτες εμπιστοσύνης και διαχείριση ρίσκου μεταξύ αλληλεξαρτώμενων υποδομών.

Πλεονεκτήματα

- SIEM και συλλογή/συσχέτιση συμβάντων: Χρησιμοποιεί Elastic Stack (Logstash, Elasticsearch, Kibana) και Επεξεργαστές Πεδίων (Domain Processors) για να συλλέγει, κανονικοποιεί και εμπλουτίζει γεγονότα από ετερογενείς πηγές, επιτρέποντας την αποδοτική συσχέτιση και ανάλυση τους.
- Χρήση AI/ML για ταξινόμηση επιθέσεων: Υποστηρίζει μηχανισμούς ανίχνευσης ανωμαλιών και κατηγοριοποίησης απειλών μέσω ML μοντέλων με δυνατότητα αναγνώρισης πολύπλοκων επιθέσεων πολλαπλών σταδίων
- Ψηφιακή εγκληματολογική διερεύνηση και τεκμηρίωση: Διαθέτει ενσωματωμένη μονάδα digital forensics που διατηρεί χρονολογικά και εμπλουτισμένα ίχνη για ανάλυση περιστατικών.
- Εμπλουτισμός συναγερμών: Η αρχιτεκτονική υποστηρίζει εμπλουτισμό δεδομένων μέσω εξωτερικών πηγών (π.χ. γεωγραφικά στοιχεία, whois, DNS, user context), βελτιώνοντας την ερμηνεία των συναγερμών.

Μειονεκτήματα

- Απουσία πλήρους συμβατότητας με διεθνή πρότυπα εμπλουτισμού (π.χ. CAPEC, MITRE ATT&CK, CVE): Αν και υπάρχει μηχανισμός εμπλουτισμού, δεν αναφέρεται ενσωμάτωση με τυποποιημένες βάσεις γνώσης, γεγονός που περιορίζει τη διαλειτουργικότητα με threat intelligence πλατφόρμες.
- Δεν παρέχεται μηχανισμός αυτοματοποιημένου εμπλουτισμού με ιστορικά δεδομένα: Η επεξεργασία γεγονότων βασίζεται σε απλούς κανόνες, χωρίς σαφή περιγραφή μηχανισμών για χρονική συσχέτιση με παλαιότερα περιστατικά

3.6.2.3 ECM [39] – Μοντέλο Ανίχνευσης Ανωμαλιών για δίκτυα OT βασισμένα σε SCADA

Το ECM (Ensemble Cybersecurity Model) αποτελεί ένα προτεινόμενο πλαίσιο κυβερνοασφάλειας για συστήματα ηλεκτρικής ενέργειας, το οποίο σχεδιάστηκε με σκοπό την ενίσχυση της ανίχνευσης ανωμαλιών σε δίκτυα λειτουργικής τεχνολογίας (OT) που υποστηρίζονται από συστήματα SCADA. Το μοντέλο επιδιώκει να προσφέρει ένα πιο ευέλικτο και ανθεκτικό σύστημα προστασίας για τα σύγχρονα κέντρα ελέγχου. Ιδιαίτερη έμφαση δίνεται στην πρόβλεψη της λειτουργικής εφικτότητας των μετρήσεων του SCADA σε επίπεδο υποσταθμού και κέντρου ελέγχου.

Η αρχιτεκτονική του ECM ενσωματώνει ένα σύστημα προβλεπτικής ανάλυσης κατάστασης (state prediction) βασισμένο σε τεχνικές μηχανικής μάθησης και ιστορικά δεδομένα λειτουργίας. Μέσω του Control Center Anomaly Detection System (CC-ADS), το μοντέλο συγκρίνει σε πραγματικό χρόνο τις τρέχουσες μετρήσεις με ένα προκαθορισμένο εύρος αποδεκτών τιμών, το οποίο υπολογίζεται με βάση προβλέψεις φορτίου, προγραμματισμένες διακοπές, τοπολογία δικτύου και αναμενόμενα σενάρια λειτουργίας. Το προτεινόμενο πλαίσιο εφαρμόζεται σε πραγματικά σενάρια λειτουργίας του δικτύου μεταφοράς και προσφέρει ένα συνδυασμό IT και OT άμυνας με στόχο την ανθεκτικότητα των συστημάτων SCADA απέναντι σε εξελιγμένες κυβερνοαπειλές.

Πλεονεκτήματα

- Το ECM ενσωματώνει λειτουργία ανίχνευσης ανωμαλιών βασισμένη σε τεχνικές τεχνητής νοημοσύνης, συνδυάζοντας ιστορικά λειτουργικά δεδομένα με προβλεπτικά μοντέλα πολλαπλών αλγορίθμων. Μέσω της πρόβλεψης του εύρους λειτουργικής αποδοχής (ensemble-based prediction) των SCADA μετρήσεων σε πραγματικό χρόνο, ενισχύεται η έγκαιρη ανίχνευση μη φυσιολογικών συμπεριφορών στο δίκτυο.
- Υποστηρίζει λειτουργίες ψηφιακής εγκληματολογικής διερεύνησης και διαφάνειας, ενσωματώνοντας μηχανισμούς blockchain για τη διαχείριση αλλαγών στη διαμόρφωση του συστήματος και την τεκμηρίωση λειτουργικών εντολών.
- Το ECM διαθέτει μηχανισμό σύγκρισης με αναμενόμενο πρότυπο λειτουργίας (Expected Operational Measurement Range – EOMR), ο οποίος δρα ως φίλτρο

πριν την ενεργοποίηση των συστημάτων συναγερμού. Αυτό προσφέρει ένα επίπεδο προληπτικής ασφάλειας.

Μειονεκτήματα

- Δεν γίνεται αναφορά σε ολοκληρωμένη χρήση εργαλείων SIEM για συσχέτιση συμβάντων από πολλαπλές πηγές (π.χ. δικτυακά logs, HMI/PLC συμβάντα), γεγονός που περιορίζει την ενοποιημένη εικόνα απειλών και την αυτοματοποίηση της απόκρισης.
- Η ενσωμάτωση εξωτερικών βάσεων γνώσης απειλών όπως το MITRE ATT&CK, CAPEC ή CVE δεν τεκμηριώνεται, με αποτέλεσμα οι συναγερμοί να μην εμπλουτίζονται με ευρύτερα συμφραζόμενα απειλών.

3.6.2.4 Συγκεντρωτική αξιολόγηση λύσεων στην διαχείριση συμβάντων ασφαλείας SCADA

Παραπάνω εξετάστηκαν προσεγγίσεις που εστιάζουν στη διαχείριση και ανάλυση συμβάντων ασφάλειας σε περιβάλλοντα SCADA. Η συγκριτική αποτίμηση βασίστηκε σε πέντε θεμελιώδη χαρακτηριστικά που θεωρούνται καθοριστικά για τη λειτουργικότητα και την αποτελεσματικότητα ενός συστήματος διαχείρισης κυβερνοσυμβάντων σε βιομηχανικά περιβάλλοντα. Τα χαρακτηριστικά αυτά περιλαμβάνουν τη χρήση εργαλείων συλλογής και συσχέτισης συμβάντων (SIEM), την αξιοποίηση τεχνικών τεχνητής νοημοσύνης για την ανίχνευση επιθέσεων, την ύπαρξη μηχανισμών ψηφιακής εγκληματολογικής διερεύνησης και τέλος, τις τεχνικές εμπλουτισμού των συναγερμών με δεδομένα από γνωστές βάσεις.

Η ανάλυση που ακολουθεί επιτρέπει τη σύγκριση μεταξύ των διαφορετικών λύσεων, αναδεικνύοντας τόσο τα τεχνικά πλεονεκτήματα όσο και τις ελλείψεις κάθε προσέγγισης. Ιδιαίτερη σημασία αποδίδεται στο κατά πόσο κάθε σύστημα δύναται να προσαρμοστεί στις ανάγκες ενός παραδοσιακού SCADA περιβάλλοντος, να ενσωματώσει σύγχρονες τεχνικές ανάλυσης και να υποστηρίξει τη λήψη αποφάσεων με βάση εμπλουτισμένα και αξιόπιστα δεδομένα. Στον πίνακα που ακολουθεί συνοψίζονται τα ευρήματα της αξιολόγησης.

Κριτήρια Αξιολόγησης	**CIPSEC**	**IADS**	**ECM**	**Παρούσα Διπλωματική**
Χρήση εργαλείων SIEM για συλλογή και συσχέτιση συμβάντων ασφαλείας	Χρήση του XL-SIEM με συσχέτιση δεδομένων από αισθητήρες και υποσυστήματα	Υλοποίηση κανονικοποίησης και ανάλυσης συμβάντων μέσω Logstash/Elastic	Όχι άμεσα SIEM, αλλά σύστημα CC-ADS για αξιολόγηση ανωμαλιών σε πραγματικό χρόνο	Υλοποίηση κεντρικού συστήματος συλλογής και ανάλυσης συμβάντων με δυνατότητες συσχέτισης
Αξιοποίηση τεχνικών τεχνητής νοημοσύνης για ανίχνευση ή ταξινόμηση επιθέσεων	Ναι, περιορισμένα μέσω Bitdefender (ML-based malware detection)	Ναι, με χρήση αλγορίθμων ML	Ναι, με προβλεπτικό μοντέλο βασισμένο σε συνδυασμό αλγορίθμων	Ναι, με αξιολόγηση διαφορετικών μεθόδων AI σε SCADA περιβάλλοντα
Υποστήριξη ψηφιακής εγκληματολογικής διερεύνησης και συλλογής αποδεικτικών στοιχείων	Υποδομές οπτικοποίησης digital forensics και συλλογή δεδομένων από honeypots	Ναι, με ενσωματωμένο εγκληματολογικό υποσύστημα	Ναι, με blockchain για αδιάβλητη καταγραφή και έλεγχο αλλαγών	Ναι, με δυνατότητα τεκμηρίωσης συμβάντων
Τεχνικές εμπλουτισμού συναγερμών από γνωστές βάσεις (CAPEC, MITRE ATT&CK, CVE)	Δεν υποστηρίζεται εμπλουτισμός από βάσεις όπως ATT&CK ή CVE	Όχι, δεν ενσωματώνονται πρότυπες βάσεις δεδομένων	Δεν γίνεται χρήση CAPEC, ATT&CK ή CVE	Προτείνεται εμπλουτισμός με πρότυπες βάσεις (CAPEC, MITRE ATT&CK, CVE)

Πίνακας 3.6-i: Συγκριτικός Πίνακας αξιολογήσεων στην διαχείριση συμβάντων ασφαλείας SCADA

4 *Συμπεράσματα και Μελλοντικές Προεκτάσεις*

Η παρούσα διπλωματική εργασία εστίασε στη μελέτη και ανάλυση των προκλήσεων της κυβερνοασφάλειας σε περιβάλλοντα SCADA, τα οποία αποτελούν τη ραχοκοκαλιά πολλών κρίσιμων υποδομών, όπως η ενέργεια, η ύδρευση και οι μεταφορές. Μέσα από μια αναλυτική θεωρητική επισκόπηση και την παρουσίαση ενός ολοκληρωμένου μοντέλου αρχιτεκτονικής, αποτυπώθηκε η ανάγκη για σύγχρονες και προσαρμοστικές προσεγγίσεις στον τομέα της προστασίας των βιομηχανικών συστημάτων ελέγχου.

Η κύρια συμβολή της εργασίας εντοπίζεται στον σχεδιασμό μιας αρχιτεκτονικής ασφάλειας που αξιοποιεί την αποκεντρωμένη επεξεργασία (μέσω εγκατάστασης SIEM agents σε επίπεδο πεδίου), την αποδοτική και κατανεμημένη αποθήκευση και ανάλυση δεδομένων (μέσω HDFS High Availability), καθώς και τη συνδυασμένη χρήση του εργαλείου Automated Forensic Tool με στόχο την αυτοματοποίηση και ενίσχυση της απόκρισης σε κυβερνοαπειλές.

Η καινοτομία της προτεινόμενης λύσης έγκειται κυρίως στην ενοποίηση διαφορετικών τεχνολογικών επιπέδων — συλλογή, ανάλυση, τεκμηρίωση και επιχειρησιακή αξιοποίηση των δεδομένων ασφαλείας — μέσα από ένα συνεκτικό πλαίσιο. Ο διαχωρισμός μεταξύ λειτουργικών δεδομένων και δεδομένων ασφαλείας, η διανομή της επεξεργασίας σε επιμέρους κόμβους και η παρουσία ενός knowledge management επιπέδου που λειτουργεί ως «δεξαμενή εμπειρίας» για την υποστήριξη του αναλυτή, ενισχύουν τη δυνατότητα πρόληψης, εντοπισμού και τεκμηριωμένης απόκρισης σε επιθέσεις.

Επιπλέον, η συγκριτική ανάλυση υπαρχουσών αρχιτεκτονικών και λύσεων διαχείρισης συμβάντων ασφαλείας ανέδειξε την απουσία μιας ολοκληρωμένης προσέγγισης που να καλύπτει ενιαία και συντονισμένα όλα τα στάδια διαχείρισης, από τη συλλογή και ανάλυση έως τον εμπλουτισμό των alerts, την τεκμηρίωση και την απόκριση. Η προτεινόμενη αρχιτεκτονική επιχειρεί να καλύψει αυτό το κενό, ενοποιώντας κατανεμημένη επεξεργασία, ανάλυση συμπεριφοράς, και διαχείριση γνώσης, με στόχο την ενίσχυση της απόκρισης και της επιχειρησιακής ετοιμότητας έναντι σύνθετων απειλών.

Παράλληλα, το σενάριο χρήσης που παρουσιάστηκε λειτουργεί ως ενδεικτικό παράδειγμα εφαρμογής της αρχιτεκτονικής, βοηθώντας στην αποσαφήνιση της

λειτουργικής ροής και της συνεργασίας μεταξύ των επιμέρους επιπέδων, από την ανίχνευση έως την απόκριση σε ένα υποθετικό περιστατικό ασφαλείας.

Η παρούσα εργασία ανοίγει τον δρόμο για περαιτέρω ερευνητική δραστηριότητα και βελτιώσεις στον σχεδιασμό συστημάτων ασφάλειας για SCADA περιβάλλοντα. Ενδεικτικά, προτείνονται οι εξής κατευθύνσεις:

- Αξιολόγηση σε πραγματικά περιβάλλοντα: Η εφαρμογή της αρχιτεκτονικής σε προσομοιωμένα ή πραγματικά SCADA περιβάλλοντα (π.χ. σε βιομηχανικούς πειραματικούς σταθμούς) θα μπορούσε να αποκαλύψει επιπλέον πλεονεκτήματα ή περιορισμούς της προσέγγισης, επιτρέποντας την περαιτέρω βελτιστοποίησή της.
- Ενσωμάτωση Μεγάλων Γλωσσικών Μοντέλων (LLMs): Η αξιοποίηση Μεγάλων Γλωσσικών Μοντέλων (LLMs) μπορεί να ενισχύσει τη διαδικασία κατανόησης και διαχείρισης περιστατικών ασφάλειας, επιτρέποντας την αυτόματη σύνοψη συμβάντων, την ταξινόμησή τους βάσει σοβαρότητας ή τύπου, καθώς και την ανάλυση των logs με στόχο την ερμηνεία της πιθανής πρόθεσης πίσω από κάθε ενέργεια. Επιπλέον, τα LLMs μπορούν να λειτουργούν ως υποστηρικτικά εργαλεία στον αναλυτή ασφαλείας, απαντώντας σε ερωτήματα ή προτείνοντας ενέργειες με βάση προηγούμενα περιστατικά.
- Αξιοποίηση τεχνικών machine learning για πρόβλεψη: Η προσθήκη προβλεπτικών μοντέλων που βασίζονται σε ιστορικά δεδομένα θα μπορούσε να δώσει τη δυνατότητα εκτίμησης κινδύνου ή πρόβλεψης πιθανών επιθέσεων με βάση τη συμπεριφορά του συστήματος.
- Διαλειτουργικότητα με εξωτερικά συστήματα: Η αρχιτεκτονική μπορεί να προσαρμοστεί ώστε να συνεργάζεται με άλλες λύσεις που εφαρμόζονται σε επίπεδο κυβερνοασφάλειας (όπως firewalls, IDS/IPS), επιτρέποντας μια ολιστική θεώρηση της ασφάλειας σε επίπεδο οργανισμού ή τομέα υποδομών.
- Ενσωμάτωση ελέγχου συμμόρφωσης: Μελλοντικά, θα μπορούσε να προστεθεί και μια λειτουργία ελέγχου συμμόρφωσης με πρότυπα (π.χ. NIST, IEC 62443), προκειμένου η αρχιτεκτονική να καλύπτει και ρυθμιστικές απαιτήσεις.

Συνολικά, η παρούσα διπλωματική εργασία ανέδειξε ότι ο συνδυασμός τεχνητής νοημοσύνης με σύγχρονες μεθόδους ανάλυσης και απόκρισης σε περιστατικά ασφάλειας μπορεί να προσφέρει μια καινοτόμα, προσαρμοστική και αποδοτική λύση για την ενίσχυση της κυβερνοασφάλειας σε περιβάλλοντα SCADA. Η προτεινόμενη

αρχιτεκτονική ενισχύει την ετοιμότητα και την ανθεκτικότητα των κρίσιμων υποδομών, προσφέροντας ένα στιβαρό υπόβαθρο για μελλοντικές επεκτάσεις και εξελίξεις, ειδικά σε έναν τομέα όπου οι απειλές συνεχώς διαφοροποιούνται και αναβαθμίζονται.

Βιβλιογραφία

[1]. Koay, Abigail & Ko, Ryan & Hettema, Hinne & Radke, Kenneth. (2022). Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. Journal of Intelligent Information Systems. 60. 1-29. 10.1007/s10844-022-00753-1.

[2]. B. Babu, T. Ijyas, Muneer P. and J. Varghese, "Security issues in SCADA based industrial control systems," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 47-51, doi: 10.1109/Anti-Cybercrime.2017.7905261.

[3]. T. Bartman and K. Carson, "Securing communications for SCADA and critical industrial systems," 2016 69th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 2016, pp. 1-10, doi: 10.1109/CPRE.2016.7914914.

[4]. Casey, E. (2011). Digital evidence and computer crime. In Forensic science, computers, and the internet. Academic Press.

[5]. Chandia, R. et al. (2007) 'Security strategies for SCADA Networks', IFIP International Federation for Information Processing, pp. 117–131. doi:10.1007/978-0-387-75462-8_9.

[6]. Eden, P. et al. (2015) 'A forensic taxonomy of SCADA systems and approach to incident response', Electronic Workshops in Computing, pp. 42–51. doi:10.14236/ewic/ics2015.5.

[7]. M. Elhoseny, H. Abbas, A. E. Hassanien, K. Muhammad and A. Kumar Sangaiah, "Secure Automated Forensic Investigation for Sustainable Critical Infrastructures Compliant with Green Computing Requirements," in IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 174-191, 1 April-June 2020, doi: 10.1109/TSUSC.2017.2782737.

[8]. M. Erol-Kantarci and H. T. Mouftah, "Smart grid forensic science: applications, challenges, and open issues," in IEEE Communications Magazine, vol. 51, no. 1, pp. 68-74, January 2013, doi: 10.1109/MCOM.2013.6400441.

[9]. Huseinovic and S. Mrdović, "Comparison of computer forensics investigation models for cloud environment," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics

(MIPRO), Opatija, Croatia, 2018, pp. 0850-0853, doi: 10.23919/MIPRO.2018.8400157.

[10]. Igure, V.M., Laughter, S.A. and Williams, R.D. (2006) 'Security issues in SCADA networks', Computers & Security, 25(7), pp. 498–506. doi:10.1016/j.cose.2006.03.001.

[11]. E. Irmak and İ. Erkek, "An overview of cyber-attack vectors on SCADA systems," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-5, doi: 10.1109/ISDFS.2018.8355379.

[12]. Kilpatrick, T. et al. (2006) 'An architecture for SCADA network forensics', IFIP Advances in Information and Communication Technology, pp. 273–285. doi:10.1007/0-387-36891-4_22.

[13]. Lallie, H.S. et al. (2021) 'Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', Computers & amp; Security, 105, doi:10.1016/j.cose.2021.102248.

[14]. Saenko and I. Kotenko, "Towards Resilient and Efficient Big Data Storage: Evaluating a SIEM Repository Based on HDFS," 2022 30th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), Valladolid, Spain, 2022, pp. 290-297, doi: 10.1109/PDP55904.2022.00051.

[15]. Navarro, J. et al. (2018) 'Huma: A Multi-layer Framework for threat analysis in a heterogeneous log environment', Foundations and Practice of Security, pp. 144–159. doi:10.1007/978-3-319-75650-9_10.

[16]. Nicholson, A. et al. (2012) 'SCADA security in the light of cyber-warfare', Computers & Security, 31(4), pp. 418–436. doi:10.1016/j.cose.2012.02.009.

[17]. M. S. Rahman, M. A. Mahmud, A. M. T. Oo and H. R. Pota, "Multi-Agent Approach for Enhancing Security of Protection Schemes in Cyber-Physical Energy Systems," in IEEE Transactions on Industrial Informatics, vol. 13, no. 2, pp. 436-447, April 2017, doi: 10.1109/TII.2016.2612645.

[18]. Romanenko, M. Tanjimuddin, P. Raussi, M. Aro, V. Tikka and S. Honkapuro, "Taxonomy of Security Threats in Energy Systems," 2020 17th International Conference on the European Energy Market (EEM), Stockholm, Sweden, 2020, pp. 1-7, doi: 10.1109/EEM49802.2020.9221940.

[19]. K. Touloumis, A. Michalitsi-Psarrou, P. Kapsalis, A. Georgiadou and D. Askounis, "Vulnerabilities Manager, a platform for linking vulnerability data sources," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 2178-2184, doi: 10.1109/BigData52589.2021.9672026.

[20]. K. Touloumis, A. Michalitsi-Psarrou, A. Georgiadou and D. Askounis, "A tool for assisting in the forensic investigation of cyber-security incidents," 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 2022, pp. 2630-2636, doi: 10.1109/BigData55660.2022.10020208.

[21]. Upadhyay, D. and Sampalli, S. (2020) 'SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability Assessment and Security Recommendations', Computers & Security, 89. doi:10.1016/j.cose.2019.101666.

[22]. Wang, W. and Lu, Z. (2013) 'Cyber security in the smart grid: Survey and challenges', Computer Networks, 57(5), pp. 1344–1371. doi:10.1016/j.comnet.2012.12.017.

[23]. Dong Wei, Yan Lu, M. Jafari, P. Skare and K. Rohde, "An integrated security system of protecting Smart Grid against cyber attacks," 2010 Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 2010, pp. 1-7, doi: 10.1109/ISGT.2010.5434767.

[24]. Wu, T. et al. (2013) 'Towards a SCADA forensics architecture', Electronic Workshops in Computing, pp. 12–21. doi:10.14236/ewic/icscsr2013.2.

[25]. Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," in IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012, doi: 10.1109/SURV.2012.010912.00035.

[26]. B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 2011, pp. 380-388, doi: 10.1109/iThings/CPSCom.2011.34.

[27]. Mahboob and J. A. Zubairi, "Securing SCADA systems with open source software," 2013 High Capacity Optical Networks and Emerging/Enabling Technologies, Magosa, Cyprus, 2013, pp. 193-198, doi: 10.1109/HONET.2013.6729785.

[28]. Ahmed, S. Obermeier, M. Naedele and G. G. Richard III, "SCADA Systems: Challenges for Forensic Investigators," in Computer, vol. 45, no. 12, pp. 44-51, Dec. 2012, doi: 10.1109/MC.2012.325

[29]. Wazuh "How it works". (n.d.). Wazuh Documentation. https://documentation.wazuh.com/current/usermanual/capabilities/vulnerability-detection/how_it_works.html

[30]. CAPEC About https://capec.mitre.org/about/index.html

[31]. CWE About https://cwe.mitre.org/about/index.html

[32]. Att&ck Resources https://attack.mitre.org/resources/

[33]. HDFS https://hadoop.apache.org/docs/r1.2.1/hdfs_desing.html

[34]. OSSIM https://cybersecurity.att.com/documentation/

[35]. Splunk https://docs.splunk.com/Documentation

[36]. QRadar https://www.ibm.com/docs/en/qsip/7.4?topic=started-qradar-overview

[37]. Álvarez, A., Trapero, R., Guilhot, D., García-Mila, I., Hernandez, F., Marín Tordera, E., Forne, J., Masip-Bruin, X., Suri, N., Heinrich, M., Katzenbeisser, S., Athanatos, M., Ioannidis, S., Kallipolitis, L., Spais, I., Fournaris, A., & Lampropoulos, K. (2022). CIPSEC-Enhancing Critical Infrastructure Protection with Innovative Security Framework. In River Publishers eBooks (pp. 129–148). https://doi.org/10.1201/9781003337492-7

[38]. S. R. Paduraru, K. S. Kshetri, S. Mohapatra, S. H. Milla, and T. Hansen, “Cybersecurity Anomaly Detection in SCADA-Assisted OT Networks Using an Ensemble-Based State Prediction Model,”National Renewable Energy Laboratory (NREL), Technical Report, NREL/TP-5R00-82591, Jan. 2023.

[39]. Motakatla, Venkateswara Reddy, Jiazi Zhang, Chen-Ching Liu, Clifton Black, Hongming Zhang, and Seong Choi. 2023. “Cybersecurity Anomaly Detection in SCADA-Assisted OT Networks Using Ensemble-Based State Prediction Model”. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-84582. https://www.nrel.gov/docs/fy23osti/84582.pdf.

[40]. Nankya, M., Chataut, R., & Akl, R. (2023). Securing Industrial control systems: components, cyber threats, and Machine Learning-Driven defense Strategies. Sensors, 23(21), 8840. https://doi.org/10.3390/s23218840

[41]. Pokane, S. S., Shilenge, M. C., & Telukdarie, A. (2022). Optimum systems integration architecture for monitoring to manage an electricity utility. South

African Journal of Information Management, 24(1). https://doi.org/10.4102/sajim.v24i1.1525

[42]. Next-Generation SCADA architectures for enhanced field automation and Real-Time remote control in oil and gas fields. (2025). International Journal of Computer Applications Technology and Research. https://doi.org/10.7753/ijcatr1112.1018